Chapter 29

Information Governance

by Ricardo Anzaldua, Taa R. Grays, Randolph A. Kahn, Lisa Douglas, and Nadia Rauf

§ 29:1 Scope note

Information is a corporate asset. Like any other asset, it needs to be appropriately managed. Information needs to be effectively and efficiently managed to advance business needs, mitigate risk, comply with legal and regulatory requirements,[1] increase employee productivity, and minimize information security and privacy threats. The effective and efficient management of information cannot occur without a strategic governing framework. This strategic governing framework is Information Governance (IG).

Information Governance, according to the Association of Corporate Counsel (ACC), "combines traditional records and information management (RIM), e-discovery, privacy, secu-

---

[Section 29:1]

[1]*See generally* Chapter 47 "Compliance" (§§ 47:1 et seq.).

rity, defensible disposition, and employee productivity into real world, executable strategies that allow organizations to better manage, retain, secure, make accessible, and dispose of their information and data through cross-functional initiatives."[2]

An Information Governance program allows a company to know where its information is and how to effectively manage it. With vast amounts of information generated on a daily basis, companies can be at risk for under-retaining or over-retaining this information. A solid Information Governance program offers not only a systematic solution to counteract risk and inefficiencies, but also allows companies to plan for the future and utilize information across many business functions to advance business interests and develop effective business strategies.[3] Without an effective Information Governance program, companies would be substantially disadvantaged in today's information-reliant environment.

This chapter will provide guidance and a roadmap to in-house and outside counsel in developing and leading a corporate Information Governance program in three parts: (1) explaining Information Governance, (2) describing how to build the strategy and program, and (3) legal and technology trends impacting Information Governance.

In Part 1,[4] the chapter lays out the key components of Information Governance. Specifically, the chapter explains key concepts, summarizes the changing business, legal and regulatory environment creating Information Governance, and discusses the broad framework for creating the program and the role of legal counsel in this Information Governance program.

In Part 2,[5] the chapter provides specific guidance and a roadmap for creating an Information Governance strategy,

---

[2]Annie Drew and Mark Diamond, Building A Business Case For An Information Governance Program, Association of Corporate Counsel (ACC) Docket, Oct. 2014, at 30.

[3]Saumya Chaki, Enterprise Information Management in Practice: Managing Data and Leveraging Profits in Today's Complex Business Environment 49 (2015). *See also* John G. Iannarelli and Michael O'Shaughnessy, Information Governance and Security: Protecting and Managing your Company's Proprietary Information 2 (2015).

[4]§§ 29:2 to 29:7.

[5]§§ 29:8 to 29:32.

an implementation plan, a governing structure, and a records retention schedule.

The legal landscape of Information Governance is evolving and will continue to shift over time. In Part 3,[6] the chapter concludes by highlighting legal and technology developments that will impact the evolution of an Information Governance strategy and program, and by providing checklists for the development, implementation, and maintenance of an Information Governance program.

§ 29:2 Objectives, concerns, preliminary considerations

The main concern addressed by an Information Governance program is to put in place a framework to holistically manage the extensive information that companies generate daily to conduct business and serve their customers. Companies possess a massive amount of information regarding the customers, employees, products and services, marketing, sales, operations, organizational structure, administration, and taxation. With the accelerating growth and use of technology, companies now have access to more information that can be extremely valuable while posing significant risk.

The objective for companies is to determine how to effectively manage and control that information in a legally compliant[1] manner in order to capitalize on the business benefits and reduce the risks. Essentially, the issue is how to *govern* that information or develop an Information Governance program.

For some, Information Governance is records management revisited. Depending on the business needs of the company, the priority may be to ensure that a functional records management program is in place.

For others, Information Governance will be broader and may be described as "the specification of decision rights and an accountability framework to encourage desirable behavior in the valuation, creation, storage, use, archival and deletion of information. It includes the processes, roles, standards

---

[6] §§ 29:33 to 29:39.

[Section 29:2]

[1] *See generally* Chapter 47 "Compliance" (§§ 47:1 et seq.).

and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals."[2] In this context, Information Governance will be a more holistic approach covering a broad spectrum of issues pertaining to information including records retention, privacy,[3] security,[4] e-signature, e-discovery,[5] etc.[6] This approach to Information Governance is becoming increasingly common as the issues that arise in these areas are complex and interrelated.

Whether a company's focus on Information Governance is narrow (records management) or broad (the governance of information), the role of the lawyer is critical. Legal counsel can help companies navigate the legal and regulatory landscape of Information Governance, provide practical business solutions, and ensure legal guidance is in line with the company's technological culture.

In developing an Information Governance program, companies should consider the following fundamental questions:

- Who owns the information?
- Who manages the information?
- Who analyzes the information?
- Is the information valuable to the company?
- Is the information required by a regulator?
- Is the information required for legal compliance, business purposes or both?
- Does the information add risk for the company?
- Does the information create new or additional legal obligations for the company?

The next three sections will introduce key Information Governance concepts,[7] examine the evolution of Information

---

[2]Debra Logan, What is Information Governance? And Why is it So Hard?, Gartner Blog Network (Jan. 11, 2010).

[3]*See* Chapter 82 "Privacy and Security" (§§ 82:1 et seq.).

[4]*See* Chapter 82 "Privacy and Security" (§§ 82:1 et seq.).

[5]*See* Chapter 81 "Electronic Discovery" (§§ 81:1 et seq.).

[6]Randolph A. Kahn and Barclay T. Blair, Information Nation: Seven Keys to Information Management Compliance, 8 (2009).

[7]*See* § 29:3.

Governance,[8] and discuss certain complexities[9] related to the Information Governance field.

§ 29:3 Objectives, concerns, preliminary considerations—Key concepts

As described earlier, Information Governance is a strategic, cross-disciplinary approach that helps organizations achieve business objectives, facilitates compliance with external requirements, and minimizes risk posed by standard information handling practices.[1] It combines traditional records and information management (RIM), e-discovery, privacy, security, defensible disposition, and employee productivity with real world, executable strategies that allow organizations to better manage, retain, secure, make accessible, and dispose of their information and data through cross-functional initiatives.[2]

Information Governance manages information, data, metadata, documents, and records to ensure that confidentiality, quality, and integrity are met for both internal and external requirements such as regulatory compliance,[3] financial reporting, data security,[4] and privacy policies.[5] Let's define some of these key concepts and terminology.

Data generally refers to symbols or characters that represent raw facts or figures and forms the basis of information.[6] It is any information stored on a computer, whether created

---

[8] *See* § 29:4.

[9] *See* § 29:5.

[Section 29:3]

[1] The Sedona Conference, The Sedona Conference Commentary on Information Management, 15 Sedona Conf. J. 125 (2014), at 3. *See also* Implementing the Generally Accepted Recordkeeping Principles (ARMA International/TR 30-2017), at 4.

[2] *See* § 29:1.

[3] *See generally* Chapter 47 "Compliance" (§§ 47:1 et seq.).

[4] *See generally* Chapter 82 "Privacy and Security" (§§ 82:1 et seq.).

[5] Saumya Chaki, Enterprise Information Management in Practice: Managing Data and Leveraging Profits in Today's Complex Business Environment 49 (2015).

[6] Implementing the Generally Accepted Recordkeeping Principles (ARMA International/TR 30-2017), at 4.

automatically by the computer, such as log files, or created by a user, such as the information entered on a spreadsheet.[7]

Information is data that has been given value through analysis, interpretation, or compilation in a meaningful form.[8]

Record is any recorded information, regardless of medium or characteristics, made or received and retained by an organization in pursuance of legal obligations or in the transaction of business.[9] It is important to understand that some information does not constitute a record such as extra copies of documents kept only for reference, publications, and library or museum materials intended solely for exhibit or reference.[10]

Records management is the field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.[11]

Records and information management (RIM) is the area of management that is responsible for establishing and implementing policies, systems, and procedures to capture, create, access, distribute, use, store, secure, retrieve, and ensure disposition of an organization's records and information.[12]

Accessibility or **access** is the right, opportunity, or means of finding, viewing, using or retrieving information.[13] This concept is especially important in circumstances where

---

[7]The Sedona Conference, The Sedona Conference Glossary: E-Discovery & Digital Information Management (4th ed. Apr. 2014), at 10.

[8]Implementing the Generally Accepted Recordkeeping Principles (ARMA International/TR 30-2017), at 3 and 5.

[9]Implementing the Generally Accepted Recordkeeping Principles at 3 and 5.

[10]Implementing the Generally Accepted Recordkeeping Principles at 4.

[11]Implementing the Generally Accepted Recordkeeping Principles at 3.

[12]Implementing the Generally Accepted Recordkeeping Principles at 5.

[13]Implementing the Generally Accepted Recordkeeping Principles at 2.

regulators require access to a company's records for audit and investigation purposes.

Deletion is the process whereby data is removed from active files and other data storage structures on computers and rendered more inaccessible except through the use of special data recovery tools designed to recover deleted data. Deletion can occur at the file level, record level, or byte level. While deletion may render the information inaccessible through the originating applications, the data is not necessarily permanently removed from the computer system. Record disposition is the final action taken in accordance with the retention schedule, concluding with destruction, transfer, or permanent preservation.[14]

Data privacy is the right to control the collection, sharing and destruction of information that can be traced to an individual.[15]

Information security is the process of protecting the confidentiality, integrity, and availability of information and assets, enabling only an approved level of access by authorized persons, and properly disposing of such information and assets when required or when eligible.[16]

Electronic discovery ("e-discovery") is the process of identifying, preserving, collecting, preparing, analyzing, reviewing, and producing electronically stored information (ESI) relevant to pending or anticipated litigation, or requested in government inquiries. E-discovery includes gathering ESI from numerous sources, reviewing and analyzing its relevance and the applicability of any privileges or

---

[14]Implementing the Generally Accepted Recordkeeping Principles at 3.

[15]Implementing the Generally Accepted Recordkeeping Principles at 3.

[16]Information security often focuses on limiting access to certain types of information that are important to the company by restricting access through various controls including physical safeguards, technical access controls, authorization challenges (*e.g.*, usernames and passwords), and encryption technologies. Information security requirements can be legally mandated (*e.g.*, Health Insurance Portability and Accountability Act (HIPPA) Security Rule), imposed by contract, industry requirements (*e.g.*, Payment Card Industry (PCI)), or by company requirements and best practices. *See generally* Implementing the Generally Accepted Recordkeeping Principles (ARMA International/TR 30-2017).

protections from disclosure,[17] and then producing it to an outside party.[18]

Electronically stored information (ESI) generally includes all information created, edited, transmitted, stored, and used in electronic form with the use of computer hardware and software.[19] ESI can include word processing files, spreadsheets, electronic versions of traditional paper documents such as PDFs, e-mail, instant messages, weblogs or "blogs," and metadata.[20]

§ 29:4 Objectives, concerns, preliminary considerations—Evolution of Information Governance

The way companies create, use, share and delete information is constantly evolving. Initially, the focus was on Records Management (RM). Information was exclusively in the form of physical documents and records stored in physical files. Later, with the development of electronic documentation, companies began to rely on electronic document management (EDM) systems. These systems involved the "process of using a computer program to manage individual

---

[17]*See generally* Chapter 33 "Attorney-Client Privilege and Attorney Work Product Protection" (§§ 33:1 et seq.).

[18]Implementing the Generally Accepted Recordkeeping Principles (ARMA International/TR 30-2017). *See generally* Chapter 81 "Electronic Discovery" (§§ 81:1 et seq.).

[19]Kenneth J. Withers, Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure, 4 Nw. J. Tech. & Intell. Prop. 171, at *9 (2006). *See generally* John H. Jessen, An Overview of ESI Storage and Retrieval, 11 Sedona Conf. J. 237 (2010); The Sedona Conference, The Sedona Conference Glossary: E-Discovery & Digital Information Management (4th ed. Apr. 2014).

[20]"Metadata" is data about data, which typically reflects the content, revisions, and management of ESI over its life cycle. *See* The Sedona Conference, The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in Electronic Age (2d ed. Nov. 2007), at 28 & n.50. *See generally* The Sedona Conference, The Sedona Conference Glossary: E-Discovery & Digital Information Management (4th ed. Apr. 2014).

unstructured files, either those created electronically or scanned to digital form from paper."[1]

With the advent of new technology that allowed for the creation of electronic records and new forms of information such as data and metadata,[2] RM evolved into Records and Information Management (RIM).[3] RIM is a broader construct involving tracking a record and information at every stage of its life from creation, use and retention, to the decision to archive or destroy the record after a determined period of time has passed. Information lifecycle management (ILM) is a term that is also used to describes "policies and procedures governing the management of data within an organization from creation through destruction."[4]

Information Governance combines all of the above and includes various legal and compliance requirements and risks addressed by different information focused disciplines, such as RIM, data privacy, information security,[5] and e-discovery.[6] A comprehensive and effective Information Governance program allows organizations to holistically and strategically manage their information to protect it against cybersecurity risks, comply with privacy requirements, keep their information accessible only to those with permission to access it, and allow users to easily find necessary information when legally required.

Developing a holistic Information Governance program is essential to managing the vast amount of information that a company possesses and interacts with at any stage of the in-

---

[Section 29:4]

[1]The Sedona Conference, The Sedona Conference Glossary: E-Discovery & Digital Information Management (4th ed. Apr. 2014), at 16.

[2]*See generally* Chapter 28 "Technology" (§§ 28:1 et seq.).

[3]Randolph A. Kahn and Barclay T. Blair, Information Nation: Seven Keys to Information Management Compliance, 24 (2009).

[4]The Sedona Conference, The Sedona Conference Glossary: E-Discovery & Digital Information Management (4th ed. Apr. 2014), at 23. *See also* Robert F. Smallwood, Managing Electronic Records, 37 (2013).

[5]*See generally* Chapter 82 "Privacy and Security" (§§ 82:1 et seq.).

[6]The Sedona Conference, The Sedona Conference Commentary on Information Management, 15 Sedona Conf. J. 125 (2014), at 3. *See generally* Chapter 81 "Electronic Discovery" (§§ 81:1 et seq.).

formation lifecycle.[7] As technology advances, more information than ever is being produced and disseminated daily. Many companies are shifting their traditional records departments into Information Governance departments that are tied more closely to other corporate functions such as privacy, information security, legal and compliance.[8] The importance of these three corporate functions to Information Governance is more fully discussed below.

Data privacy is a key and increasingly important concept in Information Governance. Data privacy principles govern the processing and transfer of personal data.[9] Data privacy is rigorously protected in many jurisdictions, particularly in European Union (EU) member states through local data protection laws and the General Data Protection Regulation (GDPR).[10] The United States has various sector specific or media-specific national privacy or data security laws, and hundreds of such laws among its 50 states and its territories. The U.S. is often perceived as less prescriptive in addressing data privacy, and lawyers are often challenged with different laws that mandate protections for specific types of data or different industry groups. For example, the HIPPA

---

[7]Saumya Chaki, Enterprise Information Management in Practice: Managing Data and Leveraging Profits in Today's Complex Business Environment 49 (2015).

[8]According to a 2016-2017 Information Governance Benchmarking Survey done by Cohasset Associates and ARMA International, the majority of companies that participated indicated that they do have a records and information management program, and many are evolving their records programs into an Information Governance program. They are making this transition because information governance is a more holistic approach to managing information than a traditional records and information management program. The survey also found that the transformation to an information governance program requires interdisciplinary participation with broad organizational collaboration. It was also revealed that a comprehensive strategy is necessary to guide information governance transformation and there must be a focus on issues such as providing support for business objectives, linking information governance to increased business performance, and setting achievable and sustainable goals for the company. *See* 2016/2017 Information Governance Benchmarking Survey, Cohasset Associates and ARMA International (Feb. 2017), at 14-15.

[9]*See generally* Chapter 82 "Privacy and Security" (§§ 82:1 et seq.).

[10]*See* Chapter 82 "Privacy and Security" (§§ 82:1 et seq.) for discussion of challenges presented by international privacy laws generally and by EU data protection standards in particular.

Privacy Rule[11] establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.[12] Several states and Puerto Rico have enacted laws that require entities to destroy, dispose of, or otherwise make personal information unreadable or undecipherable.[13] The Federal Trade Commission's Disposal Rule also requires proper disposal of information in consumer reports and records to protect against unauthorized access to or use of the information. Privacy rules tend to require businesses to keep information for only as long as necessary to serve the customer. As discussed in Section 29:5, this requirement must be balanced against business initiatives that seek to keep this information for data analytics and other legitimate business purposes.

Information security is an ongoing concern for companies, especially with the increase in cyberattacks.[14] Companies must be vigilant in regards to how the information that they retain and eventually delete is secured and protected when it includes sensitive data and personal information of customers and employees. Due to the importance of information security, companies that do not already include information security concerns as part of their Information Governance practices should consider this area as a top priority. Nearly all U.S. states have data security laws that generally require businesses that own, license, or maintain personal information about a resident of that state to implement and maintain reasonable security procedures and practices appropriate to the nature of the information and to

---

[11]*See* Chapter 55 "Employee Benefits" (§§ 55:1 et seq.) for additional discussion of the Health Insurance Portability and Accountability Act (HIPPA).

[12]*See* Chapter 55B "Health Law" (§§ 55B:1 et seq.) for discussion of employer-sponsored health care benefit programs.

[13]*See, e.g.,* Colo. Rev. Stat. Ann. § 6-1-713 and Fla. Stat. Ann. § 501.171(8).

[14]*See* Chapter 82 "Privacy and Security" (§§ 82:1 et seq.) for discussion of cybersecurity involving cyberattacks and data security incidents.

protect the personal information from unauthorized access, destruction, use, modification, or disclosure.[15]

The threat of litigation is an ongoing concern for companies. Litigation and discovery are interconnected, with a company being obliged to provide information to opposing counsel in legal proceedings. RIM principles also provide for the temporary suspension of policies or processes that might otherwise allow and result in the deletion of records or information subject to a legal hold.[16] A company's Information Governance practices must include legal hold policies and procedures to deal with the threat of litigation. Involving legal counsel familiar with Information Governance and e-discovery is essential to developing litigation policies that will save the company time and money, and potentially avoid liability when litigation arises.

§ 29:5 Objectives, concerns, preliminary considerations—Complexities

Information Governance is a complex, constantly evolving, and interconnected field. It is inherently complex due to the interplay between the legal, business and technology aspects. This section will examine three of these complexities:

- The dual nature of information.
- Conflicting retention and privacy requirements.
- Understanding the distinction between Information Governance concepts.

The dual nature of information as both an asset and a liability creates additional responsibility and complexities for a company's Information Governance strategy. Information can be an asset because it has the ability to provide value and increase business performance. For example, companies can understand market trends based on customer surveys and online purchases. Information as an asset should be managed accordingly, as a company would manage financial assets or human resources. From a risk-based perspective, companies should also understand that information may be

---

[15]*See, e.g.,* Kan. Stat. Ann. § 50-6,139b and Minn. Stat. Ann. § 325M.05.

[16]The Sedona Conference, The Sedona Conference Commentary on Information Management, 15 Sedona Conf. J. 125 (2014), at 3. *See* Chapter 81 "Electronic Discovery" (§§ 81:1 et seq.) for discussion of legal holds.

a liability, for example, in matters of privacy, information security, and litigation response. This complexity can be managed with a properly designed Information Governance program which protects companies and assists them in managing compliance issues[1] that can be vital in defending against litigation.[2]

Retaining records in accordance with statutory retention requirements while adhering to the data privacy principles that require the destruction of personal data after a specified period of time can be challenging to manage.[3] Evolving regulatory and data privacy laws further complicate matters especially for cross-border investigations that require compliance with varied, and sometimes conflicting local laws.[4] Legal counsel plays a key role in ensuring compliance with both statutory retention requirements and data privacy obligations.

Lastly, in order to develop an effective Information Governance strategy, a company must understand the distinction between Information Governance concepts. Information Governance includes many distinct concepts that are often used interchangeably. For example, there is a difference between records management, document management, and data management. Records management focuses on the records level including legal, compliance, and business considerations. Document management focuses on controls and versions of documents. Data management (sometime referred to as Master Data Management) focuses on databases and the bytes and bits that constitute the basis of information. Master Data Management (MDM) is a technology enabled business discipline in which business and IT cooperate to provide uniformity, accuracy, stewardship, semantic consistency, and accountability for an enterprise's

---

[Section 29:5]

[1]*See generally* Chapter 47 "Compliance" (§§ 47:1 et seq.).

[2]John G. Iannarelli and Michael O'Shaughnessy, Information Governance and Security: Protecting and Managing your Company's Proprietary Information 2 (2015).

[3]*See* Chapter 82 "Privacy and Security" (§§ 82:1 et seq.) for discussion of data privacy requirements.

[4]*See* Chapter 34 "Cross-Border Investigations" (§§ 34:1 et seq.).

official, shared master data assets.[5] It is important for legal counsel to understand the distinction between Information Governance concepts. Without this understanding, there is a risk that companies will fail to properly incorporate the appropriate legal, business, and technological requirements required to implement certain Information Governance practices.

§ 29:6 Navigating the legal and regulatory landscape

There are many legal and regulatory requirements that a company must consider in developing its Information Governance program including the need to address competing legal requirements. For example, statutory retention requirements may prescribe a lengthier retention period whereas data privacy legislation requires personal data of employees or customers to be retained for a shorter duration. In today's global economy it is important for companies to consider the local laws of the jurisdictions in which they operate, international laws, and industry standards.

Establishing a comprehensive legal research methodology[1] is key to ensuring that a company's Information Governance program is legally compliant on an ongoing basis. The legal research methodology will focus on local, regional, and global requirements as well as U.S. legislation that imposes recordkeeping requirements on international operations such as the Foreign Corrupt Practices Act[2] and the Foreign Account Tax Compliance Act. There will also be records retention requirements applicable to a company's activity in a specific industry, sector, or profession.

---

[5]James A. Sherer, Taylor M. Hoffman and Eugenio E. Ortiz, Merger and Acquisition Due Diligence: A Proposed Framework to Incorporate Data Privacy, Information Security, E-Discovery, and Information Governance into Due Diligence Practices, 21 Rich. J.L. & Tech 5, 38 (2015).

[Section 29:6]

[1]*See generally* Chapter 19 "Legal Research Management" (§§ 19:1 et seq.).

[2]Every issuer which has a class of securities registered pursuant to Section 78l of this title and every issuer which is required to file reports pursuant to Section 78o(d) of this title shall make and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the issuer. *See* 15 U.S.C.A. § 78m.

A comprehensive legal research methodology should consider requirements surrounding creation, content, description (attached metadata), format, interoperability, location, storage, access, security and protection, employee roles within the company charged with keeping the record, privacy maximums, cross-border transfers, exports, retention, and destruction. A company should be proactive in circumventing the risks associated with legal non-compliance, further discussed in Section 29:7, by actively engaging legal counsel in establishing the legal research methodology.

The legal landscape is not static, and legal counsel can ensure that companies maintain legal compliance on an ongoing basis by alerting the company to legal updates and assessing the impact of legal changes for the company. It is important as part of the legal research methodology to consider the frequency and timeliness of the updates in jurisdictions where an industry is heavily regulated or has onerous compliance expectations. The longer it takes for a company to become aware of relevant changes, the less time there is to comply. Sound legal research practice includes systematically evaluating resources on the basis of currency, relevance, authority, accuracy, and purpose.[3]

Navigating the legal landscape in the U.S. and on the global level can be challenging. Recordkeeping obligations will vary between jurisdictions and legislative documents. In the U.S., there are numerous laws and regulations that prescribe recordkeeping requirements for companies.[4] In conducting U.S. legal research, in addition to researching

---

[3]Meriam Library, Evaluating Information—Applying the CRAAP Test, California State University, Chico (2010), http://www.csuchico.edu/lins/handouts/eval_websites.pdf.

[4]The Internal Revenue Service requires the retention of certain accounting and tax forms. The Environmental Protection Agency mandates retention periods for discharge permits and air quality records. The Consumer Product Safety Commission requires certain manufacturers to maintain safety test records for three years. There are numerous federal laws and related regulations that impose retention requirements in specific areas such as, labor and employment and healthcare. Many times these requirements overlap and are at times inconsistent. A few examples of federal statutes imposing retention requirements for various common employment records include, the Fair Labor Standards Act (FLSA), the Family and Medical Leave Act (FMLA), the Employee Retirement Income Security Act (ERISA), and the Welfare and Pension Disclosure Act.

federal, state, and industry requirements, the following questions, among others, will need to be addressed:

- In which U.S. states does the company have operations or conduct business?
- What products and services does the company offer?
- What are the company's business entities?
- Does the company have non-profit subsidiaries (*e.g.*, a charitable foundation)?
- Does the company have Political Action Committees?
- Does the company have any known environmental liabilities for currently owned or previously owned real property?

In the U.S., there are numerous industry specific retention requirements. For example, the Health Insurance Portability and Accountability Act of 1996[5] prescribes retention obligations for health care covered entities including health care providers, health care clearing houses, and health plans. The Gramm-Leach-Bliley Act requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data.

From a risk-based perspective, it is important to identify relevant statutes of limitation during which there is a likelihood of possible claims.[6] Failure to preserve relevant documents in the face of threatened litigation can lead to severe consequences.[7] For this reason, a company should be aware of statutory limitation periods for contract and tort claims,

---

[5]*See* Chapter 55 "Employee Benefits" (§§ 55:1 et seq.) for additional discussion of the Health Insurance Portability and Accountability Act (HIPPA).

[6]State laws also provide limitations periods for other types of claims, such as those based on service contracts or business torts (*e.g.*, negligent misrepresentation or unfair trade practices). For example, in certain circumstances, an absolute limitation period may apply where there is risk of latent environmental issues arising or latent occupational diseases for which employees can bring claims against an employer.

[7]*See, e.g.,* Buonauro v. City of Berwyn, 2011 WL 3754820 (N.D. Ill. 2011) (finding that the defendant city had destroyed relevant documents with "reckless disregard" of preservation duty where deletion of audio recordings after a specified time was allowed under state law and ordering adverse inference as to content of recordings).

areas that are often heavily litigated.[8] Statutes of limitation, while not determinative of how long a record should be retained can provide useful information in establishing retention periods. For example, the Uniform Commercial Code, enacted in some form in all 50 states, provides a four-year statute of limitation in actions on sales contracts.[9]

In conducting foreign legal research, the following questions, among others, will need to be addressed:

- In which foreign jurisdictions does the company have operations or conduct business?
- What is the legal system in the foreign jurisdiction (*e.g.* civil law, common law, etc.)?
- What are the limitation periods for claims and associated litigation risks?
- What products and services does the company offer?
- What are the company's business entities?
- Are there any regional requirements to consider (*e.g.*, EU Regulations, local laws implementing EU Directives, etc.)?
- Are there any state archiving requirements?

In today's global economy, U.S. companies should also be aware of international laws or regulations which may impose additional requirements in areas such as records retention and international data transfer restrictions.[10] For example, the territorial scope of the General Data Protection Regula-

---

[8]It should be noted that while laws and regulations may impose specific retention requirements, the required retention periods should be viewed as a minimum retention period when formulating a company's document retention policy. Even when the prevailing statutory and/or regulatory regime would ordinarily permit the destruction of documents, the duty to preserve relevant documents still exists after the threat of litigation arises.

[9]U.C.C. § 2-725.

[10]The U.S. Department of Commerce and the European Commission designed the EU-U.S. Privacy Shield Framework to provide companies in the U.S. and the European Union (EU) with a mechanism to comply with data protection requirements when transferring personal data from the European Union and the United States. The EU-U.S. Privacy Shield was developed in response to the 2015 Schrems v. Data Protection Commissioner (C-362/14) case in which the European Court of Justice ruled that the Safe Harbor program was not an adequate mechanism for personal data transfer between the European Union and the United States, because of the apparent absence of sufficient protections against U.S. government

tion (GDPR), effective as of May 2018, is very broad and applicable to the processing of personal data of data subjects who are in the European Union by a controller or processor not established in the European Union.[11] This means that U.S. companies processing the personal data of European customers will be subject to the requirements of the GDPR.[12] Companies with European operations should also be aware of local laws in those jurisdictions implementing requirements for GDPR compliance.

§ 29:7 Navigating the legal and regulatory landscape—Risks

Companies that are non-compliant with their Information Governance legal and regulatory obligations may be subject to various risks, including financial harm, litigation, and loss of reputation. In the U.S. alone, there are numerous examples of cases where courts and regulators have held companies liable for not meeting their compliance obligations. Companies should understand that not all risks are created equal. As such, there may be higher risks associated with non-compliance with privacy obligations (*e.g.*, excessive retention of personal data, improper data transfers, etc.)[1] and non-compliance with regulators (*e.g.*, failure to respond to regulators, failure to produce records during audits and investigations, etc.).[2] This section of the chapter focuses on a few of these high risk areas:

- Privacy requirements related to retention and data transfers.
- Regulatory oversight and audits.

---

surveillance and corresponding redress for EU citizens. The EU-U.S. Privacy Shield addresses the shortcomings of the Safe Harbor program and provides a more stringent framework. The European Commission has deemed the EU-U.S. Privacy Shield Framework adequate to enable data transfers under EU law. *See* Chapter 82 "Privacy and Security" (§§ 82:1 et seq.) for discussion of challenges presented by international privacy laws generally and by EU data protection standards in particular.

[11]General Data Protection Regulation, Article 3.

[12]Article 30 of the General Data Protection Regulation, requires companies to maintain records of processing activities.

[Section 29:7]

[1]*See* Chapter 82 "Privacy and Security" (§§ 82:1 et seq.).

[2]*See* Chapter 67A "Regulatory Litigation" (§§ 67A:1 et seq.).

- Litigation holds and discovery.[3]
- The role of technological advances in discovery.
- Failure to train employees.

Companies often find it difficult to manage records retention requirements where there are competing privacy requirements. The General Data Protection Regulation (GDPR), mentioned in Section 29:6, is a prime example of severe financial risks that a company can incur if it fails to comply with the provisions of this regulation. Companies in breach of the GDPR can be fined up to 4% of annual global turnover or €20 million (whichever is greater).[4] There is a tiered approach to fines; for example, a company can be fined 2% of annual global turnover for not retaining its records in accordance with Article 28 of the GDPR, or for not notifying the supervising authority and data subject about a breach, or not conducting an impact assessment. Companies should be aware that GDPR rules apply to both controllers and processors, which means that cloud storage will not be exempt from GDPR enforcement.

Companies operating in highly regulated industries such as, banking and pharmaceuticals must remain especially vigilant to observe regulatory requirements. Banks in violation of the reporting and recordkeeping requirements[5] under the Bank Secrecy Act may be subject to civil penalties.[6] Similarly, manufacturers and importers of electronic products that are in violation of reporting and recordkeeping requirements under the Federal Food, Drug, and Cosmetic Act (FFDCA) may be subject to civil penalties.[7]

Litigation risks are always a looming concern for companies. Companies should ensure they have effective legal hold policies and procedures in place in order to preserve business records outside the normal records reten-

---

[3]*See* Chapter 81 "Electronic Discovery" (§§ 81:1 et seq.) for discussion of litigation holds.

[4]This is the maximum fine that can be imposed under the GDPR for the most serious infringements such as not having customer consent to process data or violating the core *Privacy by Design* concepts.

[5]*See* Chapter 53A "Financial Institutions" (§§ 53A:1 et seq.) for discussion of recordkeeping requirements of financial institutions.

[6]*See* 31 U.S.C.A. § 5321 and 31 C.F.R. § 1010.820.

[7]*See* 21 C.F.R. § 17.2.

tion schedule when faced with pending, threatened or reasonably foreseeable legal claim or litigation.[8] In *Scentsy Inc. v. B.R. Chase LLC*[9] the court expressed concern over Scentsy's inadequate retention policies and litigation hold which created uncertainty as to whether relevant documents were destroyed. Scentsy serves as a reminder that courts can and do increasingly evaluate the sufficiency of information management policies and litigation response activities.

The Information Governance leadership[10] should, therefore, develop and update policies as needed. As case law evolves, courts evolve their thinking in this space. As a result, Information Governance leadership should ensure that their policies, procedures, and directives reflect the current state of the law.[11]

A company should remain vigilant about different infor-

---

[8]In CTB, Inc. v. Hog Slat, Inc., a company failed to follow its own records retention policy which required the issuance of a legal hold. The merger of various information governance activities into a business unit augments litigation response by ensuring that regular records retention rules are suspended when a legal hold issues. Lawyers often erroneously assume that records retention schedules are enough to protect the company in the context of a lawsuit. It is important to be aware that cases can linger for years in the courts and records relevant to the matter may be destroyed during the pendency of the matter unless an effective legal hold process is imposed. Therefore, coordinating records management activities with litigation response activities makes sense for many companies. CTB, Inc. v. Hog Slat, Inc., No. 7:14-CV-157-D (E.D.N.C. Mar. 23, 2016). *See* Chapter 81 "Electronic Discovery" (§§ 81:1 et seq.) for discussion of legal holds.

[9]Scentsy, Inc. v. B.R. Chase, L.L.C., 89 Fed. R. Evid. Serv. 743 (D. Idaho 2012).

[10]*See* §§ 29:23 to 29:28 for further discussion of Information Governance leadership.

[11]*See* United Corporation v. Tutu Park Limited, 2015 WL 457853 (V.I. Super. Ct. St. Thomas Division 2015), in which the court refused to sanction a party for the disposal of information because the company had written records retention policies that allowed records to be purged in the ordinary course of business. As a result, lawyers need to ensure their companies have reasonable policies in place that are routinely being followed. Disposing of information without retention policies in place may subject the company to scrutiny as to intent or timing when information is purged. *See also* U.S. ex rel. Carter v. Bridgepoint Educ., Inc., 305 F.R.D. 225, 316 Ed. Law Rep. 896, 90 Fed. R. Serv. 3d 1836 (S.D. Cal. 2015), the court did not require the production of inaccessible data stored on backup tapes in line with changes to the Federal Rules of Civil Procedure in 2006. However, the disaster recovery personnel at many companies may perform

mation types and evolving technologies in relation to discovery.[12] Social media platforms, the Cloud, and e-communications bring a host of challenges for companies with regards to retaining internal and external communications. In *Robinson v. Jones Lang LaSalle Americas Inc.*,[13] the court clarifies that new communications and social technologies are "no principled reason to articulate different standards for the discoverability of communications through email, text message, or social media platforms." In *EEOC v. SunTrust Bank,*[14] the defendant failed to preserve surveillance camera footage in violation of its records retention policies. Lawyers can guide their organizations as more systems come online that create more and different information types. Making sure that policies are broad enough to

---

"helpful" one off retrievals of deleted documents that can undermine the lawyer's ability to assert that information was "inaccessible data." This otherwise may have been a legally acceptable basis for not producing information from backup media. If lawyers want to be in a position to assert that data is inaccessible, they need to review the company's backup policies and ensure that IT staff is not retrieving one-off documents.

[12]In Dunbar v. Google, No. C12-3305 LHK, the plaintiff sought prior versions of documents retained in the defendant's document management system. The court ordered additional discovery. This raises an important point about many technologies with greater storage capacity and functionality. The information governance policy might clarify that only the final version of any document will be retained, however technology then needs to be configured to ensure that this is actually happening. There is generally no legal requirement to retain every version of every record, but to the extent that multiple versions exist and are relevant, they may be discoverable. *See also* Marten Transport, Ltd. v. Plattform Advertising, Inc., No. 14-02464 (D. Kan., Feb. 8, 2016), in which the court refused to sanction the company for failure to retain an employee's Internet history because there was no reason to believe it would be relevant. The case also stands for the proposition that if information is not retained pursuant to a retention schedule, it still may be needed for audit, litigation or investigation if available and relevant. This further advances the idea that organizations are well served to define "information" as well as "record," as these definitions will help determine how records and non-records are managed.

[13]Robinson v. Jones Lang LaSalle Americas, Inc., 116 Fair Empl. Prac. Cas. (BNA) 193, 2012 WL 3763545 (D. Or. 2012).

[14]EEOC v. SunTrust Bank, No. 8:12-cv-1325-T-33MAP (M.D. Fla. Apr. 7, 2014).

cover new file formats and systems helps protect against discovery failures.[15]

Companies must be aware that a "lack of knowledge" of employees is not a viable defense in legal actions. Training sessions are a key component of any risk management process. In *In re: Oil Spill by the Oil Rig Deepwater Horizon in the Gulf of Mexico*,[16] the court indicted a former BP employee for obstruction of justice for deleting relevant text messages. The case further makes the point that Information Governance training efforts are essential to both educate the employee about what is expected and to inform courts, regulators, and the court of public opinion that the company cared enough about the topic to seek governance by policy. Good policies developed by coordinated Information Governance efforts help to insulate the company from the "bad" actions of employees.

§ 29:8 Importance of Information Governance strategy

An Information Governance strategy sets out the roadmap on how to manage information assets for various reasons by various parts of the enterprise with a multiplicity of business needs and legal requirements.[1] However, "[p]erhaps the key functional area that Information Governance (IG) impacts most is legal functions, since legal requirements are paramount."[2] The Information Governance strategy "is a set of guiding principles that, when communicated and adopted in the organization, generates a desired pattern of decision making. A strategy is therefore about how people throughout the organization should make decisions and allocate resources in order to accomplish key objectives. A good strategy provides a clear roadmap, consisting of a set of guiding

---

[15]*See also* Sokn v. Fieldcrest Community Unit School District No. 8, 2014 WL 201534 (C.D. Ill. 2014) (destruction of audio tape recordings).

[16]In re Oil Spill by the Oil Rig Deepwater Horizon in the Gulf of Mexico, on April 20, 2010, 87 Fed. R. Evid. Serv. 492 (E.D. La. 2012).

[Section 29:8]

[1]Robert F. Smallwood, Information Governance: Concepts, Strategies, and Best Practices, Wiley, 53 (2014).

[2]Robert F. Smallwood, Information Governance: Concepts, Strategies, and Best Practices, Wiley, 115 (2014).

principles or rules that defines the actions people in the business should take (and not take) and the things they should prioritize (and not prioritize) to achieve desired goals."[3] Without a strategy, the company makes tactical decisions that may not support the long-term goals of the organization as they relate to the management of information.

Increasingly, for example, "big data" professionals use analytics tools to crawl volumes of information to answer business questions which rely upon disparate repositories existing over time. Usually, the data that answers the business question is not known up front so proactive management is a challenge. Lawyers, privacy, and compliance professionals seek to minimize the volume of information and retention, while business professionals may want information to remain longer or forever. Such conflicts will have to be addressed as part of the overall Information Governance strategy.

§ 29:9 Building the strategy

The way the company defines Information Governance will guide the development of an Information Governance strategy. When developing a strategy, the following elements should be considered:

- Scope of the Information Governance program[1]
- Governance model including executive ownership, leadership and proper delegation[2]
- Proactive Information Governance practices[3]
- Program flexibility[4]
- Identifying existing Information Governance challenges[5]

---

[3]Michael D. Watkins, Demystifying Strategy: The What, Who, How and Why, Harvard Business Review, Sept. 2007.

[Section 29:9]

[1]*See* § 29:10.

[2]Randolph A. Kahn and Barclay T. Blair, Information Nation: Seven Keys to Information Management Compliance, xii (2013). *See* §§ 29:11 and 29:27 for further discussion on Governance.

[3]*See* § 29:12.

[4]*See* § 29:13.

[5]*See* § 29:14.

- Unearthing issues that need attention when assessing strategic objectives[6]
- Incorporating technological solutions[7]
- Framework for policies and other directives[8]
- Communications and training[9]
- Audit, monitoring, and enforcement[10]
- Implementation plan[11]
- Maintaining and continuously improving the strategy[12]

The next sections will expand on the components outlined above to guide the development of a cohesive Information Governance strategy.

§ 29:10 Building the strategy—Scope of the Information Governance program

As discussed in Section 29:2, it is essential to properly scope and define the Information Governance program prior to commencement of the strategy development efforts.[1] An Information Governance program can cover the full range of compliance issues pertaining to information including records retention, privacy, security, e-signature, e-discovery, etc.[2] In other words, if the Information Governance program is going to be nothing more than records management rather than a broader cross-functional program, this focus will substantially dictate a different strategic plan and set of activities. In this instance, the strategic plan would focus on primarily on the information management policy and re-

---

[6]*See* § 29:15.

[7]*See* § 29:16.

[8]*See* § 29:17.

[9]*See* § 29:18.

[10]*See* § 29:19.

[11]*See* § 29:20.

[12]*See* § 29:21.

[Section 29:10]

[1]Robert F. Smallwood, Information Governance: Concepts, Strategies, and Best Practices, Wiley, 65 (2014). *See also* EDRM Information Governance Reference Model, http://www.edrm.net/frameworks-and-standards/information-governance-reference-model.

[2]Randolph A. Kahn and Barclay T. Blair, Information Nation: Seven Keys to Information Management Compliance, 9 (2013).

cords retention schedule, discussed in Sections 29:29 to 29:32. No matter how Information Governance is defined, the Information Governance program should also consider and support other organizational goals and objectives.[3]

§ 29:11 Building the strategy—Governance model including executive ownership, leadership and proper delegation

An Information Governance model needs to be developed and deployed to lead the Information Governance strategy efforts, lead the implementation of the strategy,[1] and continuously improve the Information Governance program.[2] There are various governance models that can work but it is important to select a model that will fit the company's structure. Typically, Information Governance follows one of three enterprise models.

- Decentralized: (sometimes referred to as "Federated") operational activities are distributed across an organization.
- Centralized: governance and operational activities are integrated into one cohesive enterprise-wide group.
- Hybrid: a blended approach of the Decentralized and Centralized models where generally governance is centralized into one cohesive enterprise-wide group and operational activities are distributed across an organization.

These governance models are general approaches, but they can be customized or modified to meet the specific needs of an organization. Increasingly, a Hybrid model makes the most sense for most organizations.[3] Such an approach allows for unique business needs and legal requirements to be addressed.

Typically, but not always, garnering legal and IT owner-

---

[3]Robert F. Smallwood, Information Governance: Concepts, Strategies, and Best Practices, Wiley, 66 (2014).

[Section 29:11]

[1]*See* § 29:20.

[2]*See* § 29:21.

[3]Raman Mehta, IT and business alignment: Putting the federated hybrid model on steroids, CIO From IDG, May, 2015.

ship for an Information Governance program, at a minimum, is essential to increase the likelihood of success. Further, "[s]ecuring a sponsor at the executive management level is always crucial to projects and programs, and this is especially true of any strategic planning effort."[4] The governance model should include a governing board or committee that is typically led by someone with knowledge and authority to make decisions on behalf of the company on a variety of issues. Members of the board or committee should be representatives from legal, IT, privacy, security, key business representatives, and audit.

Having such a team to implement and manage the Information Governance activities not only ensures the success of the program, but can also help protect a company when litigation ensues. In *Danis vs. USN Communications, Inc*., failure on the part of executives including legal department personnel to properly implement an information management program and processes to preserve information in the context of litigation resulted in liability for the corporation as well as individuals.[5] As excerpted below, the Court admonished and held management including the CEO responsible for the company's failure to implement appropriate Information Governance processes:

> However, as the findings above made clear, the evidence establishes that Mr. Elliott was legally at "fault" for the failure to implement a suitable document preservation program. The Seventh Circuit has defined "fault" in this context as "gross negligence" or "extraordinarily poor judgment," *Marrocco,* 966 F.2d at 224—and there is plenty of evidence that Mr. Elliott's conduct falls squarely in this category.
>
> In so concluding the Court is mindful that the types of steps that must be taken to satisfy the obligation to preserve evidence may vary from case to case, based on the circumstances facing the defendant. *See generally National Hockey League,* 427 U.S. at 642 (the unique factual circumstances of a case guide a court's decision regarding sanctions). In this case, however, we believe that Mr. Elliott did not take steps to tailor

[4]Randolph A. Kahn and Barclay T. Blair, Information Nation: Seven Keys to Information Management Compliance, 53 (2013).

[5]*See also* Danis v. USN Communications, Inc., 53 Fed. R. Serv. 3d 828 (N.D. Ill. 2000).

> a plan that took into account the realities of the situation facing USN as of November 12, 1998, when this lawsuit was initiated. USN was in financial distress (Hrg. Tr. 414, 440 (Dundon)); offices were being closed and employees were leaving (*Id.,* at 414); documents (both hard copy and electronic) were being discarded as part of those office closings and employee departures (Hrg. Tr. 102, 104) (Van Dinther)); and the company had "no formal written document retention policy at USN at that time" (*Id.* at 215 (Monson)). The only policy USN had in place simply governed the preservation of documents during office closures for *business* purposes (Hrg. Tr. 249 (Elliott)), not for *litigation* purposes.
>
> Given these facts, together with the admonition by outside counsel of the critical importance of preserving documents (Hrg. Tr. 247 (Elliott)), and the Board's directive to implement a document preservation plan (*Id.*), Mr. Elliott's actions simply were insufficient, and reflected extraordinarily poor judgment. Mr. Elliott did not personally take steps to implement a comprehensive document preservation plan (Hrg. Tr. 215-216 (Monson); 247 (Elliott)). Nor did Mr. Elliott enlist outside counsel in developing and implementing such a plan: there was no request that Skadden prepare a written preservation policy (Hrg. Tr. 215, 216 (Monson)) and there were no arrangements for Skadden to meet with employees to convey specific criteria for preserving documents (*Id.*).[6]

§ 29:12 Building the strategy—Proactive Information Governance practices

The numbers of laws and regulations governing how information should be managed are increasing along with the associated risks from information mismanagement. Companies are finding proactive information management practices to be less expensive with fewer adverse ramifications in comparison to a reactive information management approach.

The increase in hacking and cybercrime incidents starkly highlights these risks. This area is one in which proactive Information Governance practices should be taken. In this context, new laws, such as the New York Department of Financial Services (NYDFS) Cybersecurity Regulation, 23 NYCRR 500, make clear that being proactive is required but substantially less costly in terms of money and reputation.

---

[6]Danis v. USN Communications, Inc., 121 F. Supp. 2d 1183, Fed. Sec. L. Rep. (CCH) P 91263 (N.D. Ill. 2000).

Focusing on the New York law for example, this regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management must take this issue seriously and be responsible for the organization's cybersecurity program and file an annual certification confirming compliance with these regulations. A regulated entity's cybersecurity program must ensure the safety and soundness of the institution and protect its customers.[1] Having an information management program in place helps the company to be "faster, better, cheaper" and "legally compliant," and allows the company to prepare for lawsuits requiring the production of electronically stored information (ESI).[2]

Similarly, as widely reported in the news, privacy failure or information security breaches today have nearly extensional impact on a company's operations and reputation and strongly militate in favor of taking significant proactive efforts to minimize the frequency of such events and their impact.[3] As discussed in The Sedona Conference Commentary on Information Governance:[4]

[Section 29:12]

[1]23 NYCRR 500, New York State Department of Financial Services, Mar. 1, 2017.

[2]Kahn Consulting, Inc., Information Management: Today's Reality, Hewlett Packard. *See* Chapter 81 "Electronic Discovery" (§§ 81:1 et seq.).

[3]*See* Chapter 82 "Privacy and Security" (§§ 82:1 et seq.).

[4]The Sedona Conference, The Sedona Conference Commentary on Information Governance, The Sedona Conference Journal, 2014, at 131.

THE INFORMATION GOVERNANCE IMPERATIVE

We live and work in an information age that is continually – and inexorably – transforming how we communicate and conduct business. Regardless of an individual organization's size, mission, marketplace or industry, information is a crucial asset for all organizations; and if inadequately controlled, a dangerous source of risk and liability.

Some examples illustrate the highly public repercussions of information control lapses:

- Significant and increasing costs of complying with e-discovery obligations;
- Data privacy and security breaches, such as a global electronics company attributing $171 million in out-of-pocket remediation costs to a data breach affecting 100 million persons, with the total harm, including reputational injury, estimated to exceed $1 billion;[6]
- E-discovery sanctions, such as an award of $8.5 million in monetary sanctions against patent holder for willfully failing to produce tens of thousands of discoverable documents;[7]
- Recordkeeping compliance penalties, such as a national clothing retailer fined over $1 million by the U.S. Immigration and Customs Enforcement Agency for information compliance deficiencies in its I-9 employment verification system, and a retail pharmacy chain reaching an $11 million settlement with the U.S. Government for record-keeping violations under the Controlled Substances Act.[8]

To minimize privacy and information security breaches, companies can be more proactive is by minimizing their information footprint. As stated in Section 29:2, companies are producing massive amounts of data and information. "Most organizations' information footprints are growing at 25-50% per year, and that is not the only challenge they face. More company information exists outside the company firewall (or in unmanaged repositories) than ever before, making control and access a new and costly complexity."[5] Information that has limited long-term value should be defensibly disposed of in a methodological manner.[6]

Information Governance programs should take the lead in helping the company defensibly dispose of unnecessary information by setting policy directives such as rules for the retention and disposition of non-records.[7] For example, "organizations may use existing software to analyze and categorize the contents of email for purposes of defensible deletion of transitory, non-substantive or non-record content."[8]

Lastly, another way companies can be more proactive is focusing on security and privacy classifications. One major issue confounding organizations globally is balancing business initiatives against privacy requirements. Lawyers need to weigh in on how to promote business "big data analytics" initiatives that seek to have more information longer against the backdrop of privacy regulations[9] that seeks to keep less for information shorter periods of time. Therefore, as part of the Information Governance activities, information security and privacy classifications become essential to proactively manage information in conformity with a variety of compet-

---

[5]Randolph A. Kahn, The Changing Information Landscape, Are You Kidding Me? Blog, Nov., 2014. *See also* Randolph A. Kahn and Breeanna T. Brock, When Information Security Became a Lawyer's Thang, ABA, Sept. 2017.

[6]Randolph A. Kahn and Galina Datskovsky, Chucking Daisies: Ten Rules for Taking Control of Your Organization's Digital Debris, ARMA International, 2013.

[7]*See* definition of "non-record" at https://www2.archivists.org/glossary/terms/n/nonrecords.

[8]The Sedona Conference, The Sedona Conference Commentary on Information Governance, The Sedona Conference, 2014, at 152.

[9]*See* Chapter 82 "Privacy and Security" (§§ 82:1 et seq.).

ing interests and to limit risk. Companies, and legal counsel specifically, should consider: "[i]n light of the characteristics of big data, and the business motivators to pursue its use, one of the most critical privacy aspects is, simply, the quality or accuracy of the data; and how an enterprise uses it might, negatively, affect an individual in decisions that are made."[10]

§ 29:13 Building the strategy—Flexibility

While the Information Governance strategy promotes consistency across the organization, it needs to be structured in a way that allows for the flexibility to comply with specific laws or regulations in each jurisdiction and different parts of the company. The strategy provides the framework for how the company should manage its information but it should not be prescriptive at a tactical level. The strategy needs be built to provide enough guidance to know what is expected but not specifically how to implement or comply.

As an example, a strategy objective may state that all records will be maintained in a company-approved records repository. However, the strategy will not tell each country, business unit, or department what repositories are approved; rather the strategy will include a process to approve repositories and established criteria for deeming a repository a company-approved records repository. Each jurisdiction may have different data handling requirements or privacy requirements with which each will need to comply and, therefore, these requirements should not be universally set for the company across all of its global operations. Many approaches and technology options can be used to satisfy the letter and the spirit of the law and accommodate business reality (funding, resources) in the context of Information Governance. Practically speaking what that may mean is utilizing different technology solutions to properly secure information in different parts of the organization even though security policy may be directed from the top. Company policies and directives must account for the fact that each juris-

[10]Lynn Goodendorf, Managing big data privacy concerns: Tactics for proactive enterprises, TechTarget, 2013.

diction may and, likely will, have different rules that must be followed.[1]

§ 29:14 Building the strategy—Identifying existing Information Governance challenges

Identifying existing Information Governance challenges should be done prior to developing an Information Governance strategy. These should be big issues that will thwart a strategy, not the smaller ones that should inform the strategy. A key Sedona Conference principle is that "[t]he strategic objectives of an organization's Information Governance program should be based upon a comprehensive assessment of information-related practices, requirements, risks, and opportunities."[1] Therefore, when embarking upon or revitalizing an Information Governance program it is essential to assess the current state of the program to risk adjust the various strategic initiatives and legal counsel should be part of this process.

In-house counsel can provide valuable guidance to proactively address these challenges. The following challenges represent a few of those experienced by companies when launching an Information Governance program:

- Location of Workforce: Understanding whether a significant portion of your workforce works from home or is mobile will help ensure that unique company can address information management challenges concerning company information outside its "care, custody or control."
- Cloud Storage: Determining if the IT department has committed to or is moving its information footprint into the Cloud helps lawyers determine special contracting needs and service level agreements (SLAs).
- Electronic Contracts: Assessing the extent to which the

[Section 29:13]

[1]For a visual illustrating one view of the differences across the globe regarding privacy regulations and enforcement laws, see Data Protection Laws of the World, DLA Piper, 2017, https://www.dlapiperdataprotection.com/.

[Section 29:14]

[1]The Sedona Conference Commentary on Information Governance, The Sedona Conference Journal, 2014, at 129.

company is using electronic contracts and electronic signatures for various business processes will help the law department work with IT to find the right contracting platform and electronic signature technology based upon the value of the business transacted and risk of breach.

- "Big Data": Understanding the extent to which analytics tools are being used to process "Big Data" helps lawyers and privacy professionals navigate the competing interests where business units may want information longer than is legally allowed or prudent from a privacy perspective.[2]
- The Transfer of Data Cross Borders: Determining if and where data is being transferred globally to ensure compliance with laws such as the EU General Data Protection Regulation (GDPR).

§ 29:15 Building the strategy—Unearthing issues that need attention when assessing strategic objectives

It is not uncommon when assessing strategic issues facing an organization to unearth an issue that needs immediate attention due to risk or potential liability. Very often these are the kinds of matters that require legal counsel involvement and immediate attention.

For example, if legal counsel learns that the technology department was implementing a new collaboration tool that failed to properly secure customer information they may need to intervene immediately to establish who can use the environment and for what information. If the technology cannot properly secure customer information, the lawyer will have to work with the business to find different technology to address its business needs.

Other issues that may need to be addressed up front include:

- Intellectual Property, Trade Secrets, PHI, PII that is in an unprotected repository or high risk cloud environment.
- Defensible disposition of information that is outdated and creates a liability.

---

[2]Randolph A. Kahn and Breeanna T. Brock, When Information Security Became a Lawyer's Thang, ABA, Sept. 2017.

- Retention of e-mail and voicemail and other eCommunications tools.
- Dealing with Discovery and volumes of old backup tapes.

§ 29:16 Building the strategy—Incorporating technological solutions

Properly managing information requires harnessing various technologies.[1] At a strategic level, decisions are being made around issues such as: cloud storage, Blockchain technology,[2] Bring Your Own Device (BYOD), and Robotic Process Automation. Because of legal implications, these decisions increasingly require the involvement of lawyers to properly guide the strategic decision. Legal counsel's advice on technology means working with technology professionals to provide a holistic solution in a way that may otherwise be disjointed. Organizations need to proactively consider legal, regulatory, privacy, and business requirements, not just end user functionality, before selecting the right technology for the organization. In other words, while in the past technology and business professionals focused largely on business need, increasingly a combination of legal, regulatory, and privacy needs also must be considered when selecting technology.

For example, "[i]n response to a shift to the Cloud as a cost-effective, scalable, storage solution, lawyers must also proactively address information ownership, access, discovery, security, privacy, and other compliance requirements in contract when negotiating with each new cloud vendor. Further, as there are many ways to implement a cloud technology solution, lawyers must become more conversant in the differences between 'public' and 'private' Clouds to be able to negotiate adequate cloud agreements."[3]

Another example, is the acceptability of electronic signatures.

[Section 29:16]

[1]*See also* Chapter 28 "Technology" (§§ 28:1 et seq.).

[2]*See* § 29:37.

[3]Randolph A. Kahn and Breeanna T. Brock, When Information Security Became a Lawyer's Thang, ABA, Sept. 2017.

§ 29:17 Building the strategy—Framework for policies and other directives

How the scope of an Information Governance program is defined[1] will guide the policy framework by dictating the topics to be covered. If the organization determines it wants a "narrow" program focusing only on records management, the Information Governance policies simply need to cover records management topics and definitions. Conversely, if the organization determines that it wants a "broad" program creating a holistic Information Governance program, then a cross-functional set of concepts (*i.e.*, security, privacy, electronic contracting, cloud storage, e-discovery, master data management, etc.) will have to be covered in various company directives.

There are certain principles underlying the creation of a company's definition of policies, procedures, and standards. Generally, policies provide a high level overview addressing Information Governance challenges such as, litigation holds, retention and destruction. Policies should require minimal change. Procedures are lower level and tactical, providing the manner in which to implement policies. Procedures require much more frequent periodic review and updates. Standards provide rules of acceptable behavior and practices that must be adhered to.

Increasingly, companies improperly meld policy directives with procedural directives. This melding is not advisable because it impacts the longevity of the directive.[2] Policy should be drafted broadly and changed as little as possible over time so that they have applicable to future business operations and technical changes. Procedures are tactical in nature and may change when business needs or technology needs change. Therefore, legal counsel need to guide the company on how to draft and implement the directives. The lawyers should assist the business in developing a defined framework to delineate policy directives from tactical procedure directives, creating the "rules" that employees are expected to follow to promote "getting it right."

[Section 29:17]

[1]*See* § 29:10.

[2]Randolph A. Kahn and Barclay T. Blair, Information Nation: Seven Keys to Information Management Compliance (2d ed. 2009).

Other areas requiring legal guidance include: helping determine who owns the company Information Governance directives, how they will be kept up-to-date, how long they will be retained after they are no longer in force, among other things.

Below is an example of a simple Information Management Policy directive and a Standard directive to demonstrate how each type of directive regulates a topic.[3] While there are many types of directive and policy constructs that can be used, each type of directive (policy, procedure, guideline, standard, etc.) should be precisely defined so that its use is consistent across the organization.[4]

Policy: *Information must be stored in a company approved records repository.*

Standard: *All records repositories must have the ability to manage records in accordance with retention event triggers.*

Procedure: *Step 1: Complete the "Records Repository Approval Form", Step 2: Submit the Form to the IG Board for review and approval . . ..*

§ 29:18 Building the strategy—Communication and training

Because communication and training[1] are so integral to an Information Governance program, determining at a strategic level how it will be done, how often employees will be trained and by whom will be essential to the program's overall success. At the strategic level, a strategic communication and training plan will be necessary to properly train employees who are not overwhelmed with information. The company will need to prioritize the topics on which employees will be trained. For example, training on information security and privacy will need to be conducted more frequently than records management. That is because information security and privacy failures typically have greater consequences and

---

[3]Randolph A. Kahn and Barclay T. Blair, Information Nation: Seven Keys to Information Management Compliance, 81 (2d ed. 2009).

[4]*See* § 29:38, which provides a framework for creating an Information Management Policy.

[Section 29:18]

[1]*See also* Chapter 38 "Continuing Legal Education and Training" (§§ 38:1 et seq.).

happen more often than records management failures.[2] For most large organizations, the development and implementation of an Information Governance program will require many important communications to be articulated from senior management including the General Counsel. So as not to overwhelm the organization, most companies have a communication plan that indicates the mode of message delivery, the timing of the message, and from whom the message will be sent. Below is an example of a communication issued by the General Counsel to all employees introducing a new Information Governance Policy.

EXAMPLE

November 27, 2017

Dear ABC Company Colleagues,

The company is augmenting its Information Governance practices to assist you in better managing Information (which includes Records and Non-Records) and to improve operational efficiency, customer satisfaction, help make more informed business decisions, as well as more easily comply with laws and regulations.

The Information Governance Policy (hyperlink) (and any related Standards and/or Procedures) provides a foundation for the management of ABC Company's Information and outlines the responsibilities that every employee shares for managing ABC Company's Information. This policy goes into effect on January 1, 2018 and you are responsible for reading, understanding and complying with the Policy.

In furtherance of this process, in the coming months, the company will be rolling out technology to help with the Information Governance efforts. If you have any concerns, questions or problems during this transition phase, please contact the IG Department or your leadership.

Records that have met their Retention Period should be properly disposed of, in accordance with the ABC Company's Records Retention Schedule. Also, please don't move or store any ABC Company Information in any unapproved location.

Remember before any information can be disposed, even if it has met its retention obligation, you need to verify that it is not under a preservation obligation, tax or audit hold or Legal Hold. Contact your leadership or the law department if you need assistance with determining if you have a preservation obligation.

If you have any questions about our policies and services, please don't hesitate to contact your leadership or the IG Department at (555) 555 - 5555.

John Smith, General Counsel
ABC Company

---

[2]Randolph A. Kahn and Barclay T. Blair, Information Nation: Seven Keys to Information Management Compliance, 92 (2d ed. 2009).

§ 29:19 Building the strategy—Compliance, audit and enforcement

The Information Governance strategy must address compliance, audit, and enforcement to ensure that the program, once implemented, is functioning as intended and that issues that arise are addressed. The only way to do that is by proactively developing a compliance, audit, and enforcement plan.[1] Below is an example of an Information Governance Audit Plan that helps an organization successfully roll out an Information Governance plan methodically and predictably by monitoring the company's progress.

[Section 29:19]

[1]United States Sentencing Commission Guidelines Manual 2016, § 8B2.1. Effective Compliance and Ethics Program, at 533.

Information Governance Level 1 Audit Plan Example

Reporting Months: [Enter Month]	U.S.	Audit	HR	IT	Legal	Europe Region	Asia Region	Manufacturing	Quality	R & D	Finance
Implementation											
Governance Structure											
Business Unit has Selected and Onboarded Team Members											
IG Business Unit Coordinators are Assigned											
IG Business Unit Coordinators are Trained											
Implementation Plan											
Implementation Plan is Customized and Drafted?											
Is the Implementation Plan Submitted for Approval?											
If There Were Open Issues, Have They All been Resolved?											
Execution of the Implementation Plan											
Are IG Communications Customized?											
Are IG Policies, Procedures, Standards Customized?											
Is the Publishing Protocol Implemented?											
Have Records Repositories been Identified and Approved?											
Has the Level 1 Audit Reporting Process Been Established?											
Has the Execution Plan Been Developed?											
Execution											
Have IG Communications been Sent to the employees?											
Have IG Policies, Procedures, Standards been Issued to the employees?											
Has IG Supplemental Training been Provided to employees?											
What Percent of Your employees have Completed the Awareness Training?											

§ 29:20 Building the strategy—Implementation plan

Building an Information Governance program can be complex, involving many business units and staff across the enterprise. To increase the likelihood of success it is essential to develop an implementation plan. Operationalizing the Information Governance strategy requires a methodical approach which is memorialized in a very detailed implementation plan. "However, creating an implementation plan is challenging. It requires the planner to identify each step required to mount a particular strategy. This activity in itself is a good test of the plan. If one does not know how to implement a given strategy, then the strategy is likely not going to be implemented."[1] The implementation plan should have tactical activities identified with associated timing and resource needs. The senior Information Governance leadership (in which the lawyers will participate) needs to own the development and management of the implementation plan. An example of an implementation plan appears below:

Activities	Timing	Resources
Implementation Plan		
Communication Plan		
Build	IG Board, Communication Manager, Communication Lawy	3 weeks
Obtain Approval	Senior Management	2 weeks
Execute Communication Plan	IG Board, Communication Manager, Communication Lawy	6 months
Training		
Identify Audiences	IG Board, Training Manager, Training Lawyer	2 weeks
Build Training Modules	IG Board, Training Manager, Training Lawyer	6 weeks
Obtain Approval	Senior Management	2 weeks
Train Employees	IG Board, Training Manager, Training Lawyer	3 months

---

[Section 29:20]

[1]Michael Kaiser, An Implementation Plan, Huffington Post, May, 2011.

§ 29:21 Building the strategy—Maintaining and continuously improving the strategy

Maintaining and continuously improving the strategy is necessary for a strategy to remain relevant in today's fast-paced and changing information landscape. An Information Governance strategy should be developed and utilized regularly. Periodically, the strategy should be re-assessed and updated as needed. It should also be realigned, as necessary, with an organization's objectives and strategic goals.[1] The Information Governance model, discussed below, will have a pivotal role in the maintenance and continuous improvement of the strategy and the program.

§ 29:22 The governing model

Information Governance is not a one time-project. It is a long-term strategy to govern the company's information and leverage the right people, the right resources, at the right time to execute the strategy. The governing model is pivotal to the successful development and execution of the strategy. This model will consist of entities and forums organizing key players and stakeholders into a collaborative team to develop and drive the strategy. Sections 29:23 to 29:27 of this chapter will flush out the details of developing the governing model to develop and drive the strategy.

§ 29:23 The governing model—Fostering collaboration to drive a successful Information Governance strategy

"Good Information Governance is like a beautiful building," explains SAP, the German business software company, "architects, builders and occupants all coming together in a common vision throughout the processes of design, construction and upkeep." Working together to achieve this shared common vision or goal – collaboration – is crucial to the success of an Information Governance program. Every corporate department has a shared interest in the common goal of strategically and proactively governing and managing the

---

[Section 29:21]

[1]Randolph A. Kahn and Barclay T. Blair, Information Nation: Seven Keys to Information Management Compliance, 229 (2d ed. 2009).

company's information. United behind this common goal, every department then has a stake in making the Information Governance program a success. Collaboration, thus, becomes the key to the success of the engine driving the Information Governance strategy.

The governing model fosters collaboration in two ways: (1) creating entities and/or forums in which cross-functional teams of associates across the company and within departments work together to understand the strategy and work together to develop the tactics to put the strategy into place; and (2) establishing processes connecting these entities/forums so they must work together to execute the strategy consistently.

The entities and forums should include: (1) a strategic planning team with senior leaders across the company who are stakeholders in the governing of information;[1] (2) tactical teams for each department consisting of leaders, managers and individual contributors who are a combination of stakeholders and key players in executing, embedding and ensuring compliance with the Information Governance program at the department level;[2] (3) individual contributors who support the tactical team by executing the program at the associate level;[3] and (4) a program office consisting of a dedicated team of Information Governance professionals who support the governing structure and manage the day to day operations of the Information Governance program.[4]

The processes should include: (1) monitoring compliance with the program; (2) decision-making to execute strategic components; (3) escalating issues, problems and matters that can impact the entire program; and (4) program office support for the governing structure. These processes create the foundation and foster the need for collaboration within and across departments. This collaboration creates relationships within and across the departments that will continue to drive the engine of the governing structure to sustain the governing and managing of information in the company.

[Section 29:23]

[1] *See* § 29:24 for discussion of how to identify those stakeholders.

[2] *See* § 29:25.

[3] *See* § 29:26.

[4] *See* § 29:27.

The entities/forums and the processes forge foundational relationships within and between departments that will ensure the long-term success of the program.

§ 29:24 The governing model—Identifying key players and stakeholders

"The proper management of information requires across-functional collaboration."[1] The success of the Information Governance program rests on identifying and empowering a cadre of associates from across the company. This group consists of two types of associates: stakeholders and key players. Stakeholders are business units and teams whose business activities drive information use or impact information use. Key players are those who are pivotal to the execution of the Information Governance strategy. Some of the entities/forums will consist solely of one group or the other as well as a mix of both groups.

Although each entity and forum will need different stakeholders, these general questions can be used to initially identify the key stakeholders:

- What information drives your company's business?
- What information is subject to regulation and is the focus of litigation?
- Which departments are responsible for creating or handling this information?
- Within these departments, who is responsible for executing the company's strategy?
- Does this person have influence with other leaders in the department to drive the execution of the company's strategy?
- Does this person have decision-making authority in executing the strategy (allocating department funds, people and process)?

Legal will be one of these key stakeholders. According to a Corporate Executive Board (CEB) survey, "Legal, more than any other department, is likely to provide support to Infor-

---

[Section 29:24]

[1]Corporate Executive Board, Manage Risk with Information Governance, http://www.cebglobal.com/member/legal/blog/16/manage-risk-with-information-governance.

mation Governance . . . and typically, the GC will be a core participant in an Information Governance committee or team."[2] Legal brings several perspectives to the development of the program: (1) experience of the pain of poor information management due to litigation/regulatory inquiries; (2) owner of many aspects of key Information Governance policies; (3) a focus on helping the company avoid risk; and (4) a respected voice with senior management.[3]

Although each entity and forum will need different key stakeholders, these questions may be used to initially identify the key players for the Information Governance program:

1. What processes need to be created, modified, enhanced, or eliminated to execute the strategy?
2. Which department owns these processes?
3. Who in the department owns these processes?
4. Who in the department funds these processes?
5. What tools (applications, systems) are needed to execute the program?
6. Who owns these tools? Are they jointly owned?
7. Which team is or teams are responsible for these tools?
8. Who are the people that are the administrators or specific owners of these tools? Tools can have an IT owner and a business owner.

§ 29:25 The governing model—The governing board/committee embedding collaboration into the strategy

The first key entity to create is the governing board/committee. It is a strategic planning team with senior leaders across the company who are stakeholders in the governance of information. As described earlier, the governing board/committee will be a cross functional team of leaders

---

[2]Corporate Executive Board, Manage Risk with Information Governance, http://www.cebglobal.com/member/legal/blog/16/manage-risk-with-information-governance.

[3]Contoural, Infopak: Information Governance Primer for In-House Counsel, http://www.ACC.com, at 16.

from across the corporation.[1] "Cross-functional committees or informal working groups are the most commonly used structures to address Information Governance initiatives."[2] According to a 2015 Corporate Executive Board (CEB) survey of its members on Information Governance management structure, over 40% of its surveyed members have cross—functional committees or informal working groups.[3]

Many companies struggle with fostering collaboration in the way their teams work. Collaborative efforts tend to fail for many reasons: "competitive self-interest, a lack of a fully shared purpose and a shortage of trust."[4] Collaboration is a must for an Information Governance strategy: all stakeholders must work together to create a unified goal and allocate resources from across the corporation to achieve this goal. The governing board/committee, therefore, must embed the three cornerstones of collaboration in the strategy:

- *Transparency*: "A lack of hidden agenda or conditions, accompanied by the availability of full information required for collaboration, cooperation and collective decision-making."[5] Clear communication about what needs to be done and who is responsible for those tasks ensures success.
- *Accountability*: Every department is involved in the development of strategy, has a role in ensuring it is successfully executed and will be held responsible for not doing its share of the work.

[Section 29:25]

[1]*See* § 29:24.

[2]Information Governance Benchmark Report, Corporate Executive Board – Leadership Council for Legal Executives, http://www.cebglobal.com, at 14.

[3]The survey results were: 24%—formal cross-functional teams, 20%—informal group of stakeholders that collaborate, 12%—a team or group of stakeholders within a function, 12%—independent structures, 14%—each function executes a program independently, and 18%—do not have any structure. *See* Information Governance Benchmark Report, Corporate Executive Board – Leadership Council for Legal Executives, https://www.cebglobal.com, at 14.

[4]Ram Nidumolu and Jib Ellison et al., The Collaboration Imperative, Harvard Business Review, Apr. 2014.

[5]*See* Business Dictionary, http://www.businessdictionary.com/definition/transparency.html.

- *Cooperation*: everyone understands that they must proactively work together for the common goal, sharing needed information, supporting each other in the work that needs to be done and removing roadblocks and obstacles impeding the execution of the program.

In addition to developing the strategy, this team has several other key governance responsibilities: (1) developing the implementation plan for the Information Governance strategy;[6] (2) monitoring the progress of the implementation plan; (3) serving as an escalation point for issues arising from implementation; (4) keeping the strategy current by periodically reviewing and updating it; (5) holding the tactical teams and fellow stakeholders accountable for the continuing success of the program; and (6) serving as ambassadors to explain the business and risk mitigation value of Information Governance.

§ 29:26 The governing model—The tactical teams that drive implementation of the strategy and ongoing maintenance

Once the governing board/committee establishes the strategy and develops the implementation plan,[1] it has to be executed. The entities/forums responsible for implementing the Information Governance strategy are the tactical teams.

These teams will consist of stakeholders and key players who will embed the Information Governance program into the company. As at the strategic level, collaboration is pivotal at the tactical level. The teams are responsible for translating the implementation plan into concrete tasks and executing those tasks. They must cooperatively work together to align, deploy and share resources to achieve the unified goal.

As described earlier,[2] the governing board/committee develops the implementation plan. Key components of that plan impacting the tactical team are: (1) deciding what type of tactical teams are needed – by department, implementa-

---

[6] *See* § 29:20.

[Section 29:26]

[1] *See* § 29:25.

[2] *See* § 29:25.

tion activities, strategic goals; and (2) selecting or facilitating the selection of leaders and key players for each of the tactical teams.

The tactical teams must identify, align and manage the people, processes and tools to implement the Information Governance strategy. The roles of the people, processes and tools will vary depending on the purpose of the tactical teams. Generally, the teams will be responsible for: (1) aligning with the Information Governance directives – policy, standards, processes and procedures[3] – and identifying what existing policies, standards, processes and procedures need to be modified to align to the strategy; (2) identifying what tools need to be modified or no longer used to support the program; (3) developing a communication plan to socialize the Information Governance activities;[4] (4) developing training programs to educate associates on the Information Governance program and their responsibilities;[5] (5) assigning individuals and teams to execute these tasks; and (6) monitoring the status of the implementation and holding leaders and key players accountable for delivering on their tasks.[6]

Once the strategy is implemented, these teams, or some version of them, will need to remain in place to ensure that the Information Governance program is embedded in the day-to-day work of the corporation at the department and associate level. These teams also ensure that the program remains flexible and adaptable to the needs of the business and corporate functions. These teams will (1) measure corporate compliance with the Information Governance program; (2) determine how business changes (onboarding new tools, selling off or acquiring new businesses) will impact the program and if modifications to the program need to be made; (3) determine if regulatory/legal changes that impact the way business is conducted will require changes to the program; (4) escalate issues or concerns that pose risk to the success of the program to the governing board/committee; and (5) partner with the Information Governance program

---

[3]*See* § 29:17.

[4]*See* § 29:18.

[5]*See* § 29:18.

[6]*See* § 29:19.

office[7] to support the teams' day-to-day management of the program.

§ 29:27 The governing model—The Program Office which manages the Information Governance program day to day

A key component of the governing structure is the team that manages the program on a daily basis. This team is the Program Office. It consists of Information Governance professionals with subject matter knowledge in technology, legal, compliance, information management, and an understanding of the company's business.[1]

The team has several responsibilities:

1. Liaise with the strategic and tactical teams serving as the team's point person for Information Governance questions, comments, concerns and guidance.
2. Keep the policy, standards, processes, and procedures current.
3. Work collaboratively with the key players to ensure the program is implemented and regularly updated to get ahead of changes or new initiatives that can impact the program.
4. Develop training for associates and members of the governing model to establish a baseline of understanding about Information Governance and keep all employees informed of important changes in the program.
5. Develop audit and compliance standards.

§ 29:28 The role of legal counsel in Information Governance

Due to the increasing complexity of legal requirements, technology, and data which form the basis for records management infrastructure, it is more important than ever that counsel take on the responsibility of scrutinizing legal research and opinions. Legal counsel should form part of the

---

[7]*See* § 29:27.

[Section 29:27]

[1]*See* Contoural, Identifying and Hiring IG Talent, https://www.acc.com, for details about how to assemble a team to staff your Information Governance Program.

tactical team that drives the implementation of a company's Information Governance strategy and ensures ongoing compliance.[1] Legal counsel can be involved in the development and implementation of a company's Information Governance strategy as follows:

1. Develop an Information Governance program that post-implementation continues to be legally compliant:
   - Review existing records retention policies and schedules for legal acceptability.[2]
   - Ensure the appropriate stakeholders are notified of applicable legal developments.
   - Assess and update the Information Governance strategy based on legal updates and regulatory requirements.
   - Ensure that privacy laws and regulations in relation to the retention of personal data are incorporated into the Information Governance strategy.
2. Develop an Information Governance program that is cost-efficient and risk-averse:
   - Conduct a risk assessment periodically based on legal and regulatory compliance requirements and updates.
   - Optimize costs by retaining information for only as long as necessary to meet legal or business purposes.
   - Reduce inefficiencies and decrease storage costs by identifying non-records that do not require retention and establish destruction protocols.
3. Develop policies and procedures to ensure that the following objectives are met:
   - Valuable information is reliably and readily accessible.
   - Confidential and proprietary information is protected.
   - Personal data is safeguarded against unlawful access.

[Section 29:28]

[1]*See* § 29:26.

[2]William Saffady, The Business Case for Records Management, ARMA Intl. Information Management J, Nov.-Dec. 2016, at B-51. *See* §§ 29:29 to 29:32 for discussion of records retention policies and schedules.

- Appropriate litigation hold policies are in place.
- Appropriate retention and destruction policies are in place.

Identifying and managing records that are currently unaccounted for by a company's Information Governance program will require a multi-disciplinary approach with a wide range of internal stakeholders who collaborate to build bridges across corporate information silos. The need for counsel to actively engage with other stakeholders and provide adequate legal infrastructure supporting the practice has never been higher.

§ 29:29 The records retention schedule

Companies are challenged with controlling the volume of information that they create, use and share, while ensuring that their records are retained in accordance with legal and regulatory requirements in addition to business needs.[1] The disposition of records is not as straightforward as physically destroying them or deleting them from electronic storage as space runs out.[2] The ability to effectively find and secure the right information is dependent on the proper management of a company's records. This mandate is accomplished through the establishment of an Information Governance strategy and program. The records retention schedule[3] is a foundational element of a successful Information Governance program.

For Information Governance programs focused narrowly on records management, the records retention schedule will take center stage. For more holistic Information Governance programs, the records retention schedule will be one of many

---

[Section 29:29]

[1]Nancy D. Barnes, Jeff Whited and Vicki Wiler (eds.), Implementing the Generally Accepted Recordkeeping Principles (Overland Park, KS: ARMA International, 2017), at 24.

[2]John C. Montana, What a Records Retention Schedule Is—And Why You Need One, Information Management Journal 50, no. 2 (2016), at B-2.

[3]A records retention schedule is a policy instrument that governs the creation, retention, and destruction of all business records of a company. *See* Tina Torres, Creating a Process-Focused Retention Schedule, Information Management Journal 40, no. 5 (2006), at 62.

key considerations.[4] Regardless of the scope of a company's Information Governance program, the records retention schedule will remain an important element. The next sections of this chapter will discuss:

- Why is the records retention schedule required (Philosophy)?[5]
- What are the key elements of the records retention schedule (Scope)?[6]
- What is required to build and keep the records retention schedule (Planning, Development, and Maintenance)?[7]

§ 29:30 The records retention schedule—Philosophy

All companies generate and use records. The management of records can be a monumental undertaking for any company, especially if it has global operations and is part of a highly regulated industry. A company may have thousands of record types governed by a multitude of laws with different jurisdictional requirements and regulatory compliance obligations.

The records retention schedule resolves the issues that companies come across in managing records by providing a straightforward solution to properly document business activities and satisfy legal and regulatory requirements.[1] By accommodating all of a company's recordkeeping needs, a records retention schedule provides a "one stop shop" for its users.

Records have a lifecycle which starts at creation and ends at the final disposition of the record. The core purpose of a records retention schedule is to list which records are created and maintained by a company and how long the

---

[4]*See* § 29:2 for discussion of narrow and holistic approaches to information governance.

[5]*See* § 29:30.

[6]*See* § 29:31.

[7]*See* § 29:32.

[Section 29:30]

[1]Tina Torres, Creating a Process-Focused Retention Schedule, Information Management Journal 40, no. 5 (2006), at 62.

company must keep each record.[2] Business records hold value for a company's operations and play a vital role in the management of the company. The value of business records varies, therefore, a company must ensure that there are systems in place to classify and retain the right types of records. A company's inability to locate valuable business records will impede the progress of its business operations and create risk of liability. The records retention schedule allows companies to classify and store business records based on value and legal requirements.

Technological advances allow for the rapid creation and distribution of information. With these advances, business practices also need to evolve. A company cannot afford to sideline the records retention schedule component of its Information Governance strategy.

§ 29:31 The records retention schedule—Scope

Records retention schedules outline which information must be retained as a record, for how long, and when to dispose of it when the record is no longer required.[1] A records retention schedule accounts for the record lifecycle as well as performing the following functions:

- Ensures the retention of the records and information necessary for the efficient operation of the business.
- Demonstrates compliance with the applicable legal and

---

[2]John C. Montana, What a Records Retention Schedule Is and Why You Need One, Information Management Journal 50, no. 2 (2016), at B-2. *See also* Society of American Archivists, A Glossary of Archival and Records Terminology, http://www2.archivists.org/glossary/terms/r/record. A business record is any document or data that records a company's business activities or decisions. Records exist in many forms, including hardcopy, digital, text, images, graphs, sound, video, and any other medium from which information can be obtained. However, the concept of the record is independent from its format. For example, a digital copy of a hardcopy record, such as a receipt, contains the same information as the original. A records retention schedule applies to all records created and maintained by a company, regardless of format.

[Section 29:31]

[1]Nancy D. Barnes, Jeff Whited and Vicki Wiler (eds.), Implementing the Generally Accepted Recordkeeping Principles (Overland Park, KS: ARMA International, 2017), at 24. The foundation of any records retention schedule includes the following components: business function; record class, series or category; record or document types; and retention periods.

regulatory requirements in the jurisdictions in which a company operates.

- Defends a company from liability through identifying the records required for audits, investigations, litigation or other legal proceedings.
- Reduces recordkeeping burdens and the costs associated with the maintenance and storage of records for longer than necessary.

§ 29:32 The records retention schedule—Planning, development, and maintenance

During the planning stage for the records retention schedule there are a number of considerations that must be taken into account which include the following elements:

- Understanding the scope of business operations and applicable jurisdictions to determine which laws and regulations apply to the company's recordkeeping requirements.
- Reviewing the company's legacy schedule, if available, to determine how record types were previously mapped. This exercise can inform the structure of the schedule and provide an understanding of how a company classifies its record types.[1]
- Collecting details on the company's records through interviews with key stakeholders within the company and/or standardized questionnaires distributed to key users of the schedule.[2]
- Identifying key stakeholders, including legal counsel and records management personnel, who will be compiling the legal research and ensuring the schedule encompasses all of the applicable legal retention requirements.[3]

It is not possible to apply a one-sizes-fits-all schedule to a

---

[Section 29:32]

[1]Laurie Fischer, Condition Critical: Developing Records Retention Schedules, Information Management Journal 40, no. 1 (2006), at 27.

[2]Laurie Fischer, Condition Critical: Developing Records Retention Schedules, Information Management Journal 40, no. 1 (2006), at 27.

[3]Laurie Fischer, Condition Critical: Developing Records Retention Schedules, Information Management Journal 40, no. 1 (2006), at 27.

company. Companies that operate in the U.S. and abroad should reconsider using a U.S. focused records retention schedule during the planning stage. Issues that may arise through the use of a U.S. centric retention schedule include the following:

- Legal requirements of other applicable jurisdictions will not be accounted for which may create non-compliance risks in these jurisdictions including from the perspective of data privacy compliance.[4]
- Records types will be identified through the use of U.S. centric terms which will lose meaning for non-U.S. operations that are seeking to implement the retention schedule and policies, resulting in further compliance challenges.[5]

During the development of the records retention schedule, information regarding the types of records that each department processes, creates, receives and maintains must be collected.[6] It is important that the users are able to associate their records with the retention schedule.[7] Information regarding the format of the records, the physical space that records occupy, the frequency in which records are accessed, and current retention practices should also be collected.[8] This information establishes the core of the retention schedule by ascertaining business functions, record classes, series or categories, and record types or examples. Once this step is completed, recordkeeping requirements are mapped into the retention schedule. The duration for which records must be retained ("retention period") and the event trigger ("retention event") can be driven by legal and regulatory require-

---

[4]Laurie Fischer, Condition Critical: Developing Records Retention Schedules, Information Management Journal 40, no. 1 (2006), at 26.

[5]Tim Corey, Tips for Globalizing a U.S.-Based Records Retention Schedule, Information Management, ARMA, Nov.-Dec. 2016, at 26 (discussion of I-9, ERISA 5500, and IRS 1099 forms).

[6]Laurie Fischer, Condition Critical: Developing Records Retention Schedules, Information Management Journal 40, no. 1 (2006), at 30.

[7]Tina Torres, Creating a Process-Focused Retention Schedule, Information Management Journal 40, no. 5 (2006), at 66.

[8]Laurie Fischer, Condition Critical: Developing Records Retention Schedules, Information Management Journal 40, no. 1 (2006), at 32.

ments, statutes of limitations,[9] or industry best practices. Once the retention periods and events for all record classes have been validated from a legal and business perspective, the retention schedule is complete.

Retention schedules are not static documents. The Information Governance Program office and the appropriate stakeholders and key players, including legal counsel, should review the retention schedule regularly. In that regard, it is useful to seek to simplify schedules in part by coalescing categories to have fewer retention rules which augments compliance. Further, retention schedules require regular refreshes and updates to ensure currency with changing business practices, technologies, and laws.[10] Corporate acquisitions, reorganizations, expansions, as well as new products, services, territories and business lines can impact the currency, functionality and compliance of the retention schedule. Laws and regulations may be created, updated, or repealed which in turn affects recordkeeping requirements. Schedule refreshes and reviews are particularly vital for large companies that operate in complex legal environments. During the planning, development, and maintenance stages of the retention schedule, the role of legal counsel is essential to ensure the schedule is and remains legally compliant on an ongoing basis.

---

[9]The application of limitation periods to a records retention schedule should be carefully thought out, especially when determining a retention period because the length of a limitation period may far exceed relevant privacy maximums. Privacy maximums refer to the obligation to retain personal data for a specific period of time after which the personal data must be destroyed. Limitation periods should only be applied to categories where there is a rational connection between the context and the likelihood of a dispute that may arise after any applicable statutory retention period has expired. Furthermore, as noted above, a legal hold process must be designed to retain records necessary in the event of claims, litigation, and similar proceedings, outside the context of the normal retention schedule. Many companies over-retain records on the basis of limitation periods which are costly and create risk from the perspective of compliance with privacy laws as well as leaving companies open to potential embarrassment and legal risk should the records become subject to discovery.

[10]Susan Cisco, Big Buckets for Simplifying Records Retention Schedules, 42:5 ARMA Intl. Information Management J. (2008), at 5. In 2008, ARMA recommended an 18-24 month refresh cycle for organizations operating in highly regulated industries.

§ 29:33 Trends

Information Governance for legal practitioners is not only about managing today's complexities. It is also about keeping focused on the horizon for technological changes and legal developments. Although the pace of legal change may not be in step with advancing technologies, the legal landscape is evolving dramatically and quickly. Recent developments such as Blockchain technology,[1] the Internet of Things (IoT), electronic medical records, smart cars, and drones have required legal practitioners to delve into new areas of Information Governance.[2] The topics discussed in Sections 29:34 to 29:37 of this chapter represent a few issues on the Information Governance horizon. It is important to keep in mind that these developments can be expected to evolve, change, and be replaced by new concerns. Legal counsel is well advised to stay ahead of emerging technologies, new laws and regulations, and their impact on Information Governance.

§ 29:34 Trends—Legislating information

Legislators are regulating the various ways that information needs to be managed and no longer leaving its management to chance. Whether in regard to retention,[1] privacy, information security,[2] or any other aspect of Information Governance, there is a growing body of laws and regulations that prescribe the way information must be managed and the consequences of failure.

As an example, for a heavily regulated global organization operating in dozens of jurisdictions around the world, the number of applicable requirements could easily number in the thousands for purposes of records retention alone. Similarly, when trying to manage privacy across a global

---

[Section 29:33]

[1]*See* § 29:37.

[2]Randolph Kahn, Law's Great Leap Forward: How Law Found a Way to Keep Pace with Disruptive Technological Change, American Bar Association (ABA), Nov. 2016.

[Section 29:34]

[1]*See* §§ 29:29 to 29:32.

[2]*See generally* Chapter 82 "Privacy and Security" (§§ 82:1 et seq.).

company, the regulations in every state in the U.S. may be relevant as well as each jurisdiction internationally.

Lawyers should expect to see more laws, regulations and industry standards in most jurisdictions that address privacy, secure disposal, encryption of data, records retention, e-mail management, secure transmission, information security, etc. The holistic Information Governance approach to managing information can help to develop a consistent and routinized way for organizations to deal with new rules mandated in these various areas.

§ 29:35 Trends—Cloud storage

Increasingly, organizations are storing their information in various cloud providers' environments because it is a cost-effective and scalable option.[1] "The worldwide public cloud services market is projected to grow "18 percent in 2017 to total $246.8 billion, up from $209.2 billion in 2016," according to Gartner, Inc.[2] Legal counsel should be involved up front in vetting storage options to make sure their Information Governance needs are being addressed. During the contracting process, counsel should address information ownership, access, discovery, security, privacy,[3] and other compliance requirements. Further, lawyers must become more knowledgeable on the differences between the types of Clouds (*i.e.*, public, hybrid, private) so they can address unique requirements as they arise.

§ 29:36 Trends—Safeguarding information with outside counsel

Equally important as managing the information within a company is managing the company information held by vendors outside the company. Outside counsel firms, as compared to the other vendors, are privy to far more

---

[Section 29:35]

[1]*See* Chapter 49 "Corporate Information Technology Transactions and Disputes" (§§ 49:1 et seq.) for discussion of cloud-based services.

[2]Gartner, Gartner Says Worldwide Public Cloud Services Market to Grow 18 Percent in 2017 (Feb. 22, 2017), https://www.gartner.com/newsroom/id/3616417.

[3]*See generally* Chapter 82 "Privacy and Security" (§§ 82:1 et seq.).

confidential and business sensitive information.[1] Because of the copious amounts of confidential and sensitive information they hold, law firms have become prime targets of hackers. This trend does not show signs of abating.[2] This is especially important when using third-party collaboration tools that likely store information outside the firewall of both the company and the law firm which may pose greater information security challenges. In other words, inside counsel need to not only manage what their outside law firm does with their information but also select and manage proper technology that securely augments the legal collaboration process.[3]

A company's Information Governance directives should inform in-house lawyers how to manage relationship with all

---

[Section 29:36]

[1]"First as vendors, law firms are attractive targets," explains Luke Dembosky, a cybersecurity and litigation partner at Debevoise & Plimpton. "They not only hold valuable client information but also are regularly e-mailing attachments to clients, providing a possible means to get into client systems. . . . Second, law firms are seen . . . as high-value targets for the rapidly growing use of 'ransomware' and extortion schemes because they have historically weak defenses and are seen as able to pay large sums." Julie Sobowale, Law Firms must manage cybersecurity risk, ABA Journal, Mar. 2017. *See also* Matt Neely, Law Firm Hackings on the Rise: Why Should You Care and What Should You Do?, http://www.securestate.com/blog/2017/01/13; Stephen Treglia, Increasing Cybersecurity Requirements for Lawyers, New York Law Journal, May 30, 2017; Helen Gunnarsson, Humans Make Law Firms Vulnerable to Cyber Attacks, Lawyer Says, Bloomberg BNA, http://www.bna.com/humans-law-firms-n57982085616.

[2]On November 1, 2009, the FBI issued its first advisory warning law firms of " 'noticeable increases' in efforts to hack into [their] computer systems." *See* Lolita Baldor, FBI: hackers targeting law and PR firms, NBCNEWS.com, Nov. 17, 2009. On January 31, 2013, speaking at LegalTech's annual conference, Mary Galligan, Special Agent in charge of cyber and special operations, of the FBI's New York Office stated, "We have hundreds of law firms that we see increasingly being targeted by hackers." *See* Evan Koblentz, LegalTech Day Three: FBI Security Expert Urges Law Firm Caution, LegaltechNews, http://www.law.com/legaltechnews/almID/1202586539710/?slreturn=20170923121206. On December 27, 2016, the U.S. Attorney for the Southern District of NY announced the indictment of three Chinese nationals charging them with hacking into two prominent law firms. *See* Press Release, U.S. Attorney's Office (SDNY), Dec. 27, 2016.

[3]Aebra Coe, Why Big Law May Be In Big Trouble After Data Breaches, Law 360, Mar. 31, 2016.

vendors – especially outside counsel – and how the vendors manage the company's information. In-house and outside counsel must work closely to safeguard corporate information so law firms can meet their ethical obligations,[4] and to ensure that companies can minimize the risk of their confidential and sensitive information being stolen by hackers.[5]

§ 29:37 Trends—Blockchain

Blockchain is a distributed ledger technology,[1] which has considerable appeal in the Information Governance space. In particular, its potential as a way of creating, maintaining,

---

[4]With the ever changing technology attorneys use to service their clients, lawyers' ethical obligation to protect client confidences becomes fraught with greater risk of unintentional or deliberate disclosures. The ABA has provided guidance on how to meet their ethical obligations: ABA Rule Comment 8 to Model Rule 1.1—Competence: Lawyers are to keep abreast of changes, including the benefits and risks associated with relevant technology; ABA Formal Opinion 99-413: Protecting the Confidentiality of Unencrypted E-mail; ABA Formal Opinion 477R: Securing Communication of Protected Client Information; and ABA Formal Opinion 11-459: Duty to Protect the Confidentiality of E-mail Communications with One's Client (warning clients of the risk of sending/receiving client information electronically, where there is a risk a third party may gain access). *See* Chapter 31 "Ethics" (§§ 31:1 et seq.) for discussion of the lawyer's ethical duty to protect confidential information.

[5]For law firms, corporations should apply their Information Governance programs in the following ways: (1) include in outside counsel policy statements or retention agreements the corporation's expectations for the law firm to safeguard its information; (2) have the law firm undergo a security assessment and work with the firm to resolve the risk findings that may arise; and (3) conduct training with key members of the law firm concerning your corporation's information governance policies, standards, procedures and standards.

[Section 29:37]

[1]Distributed ledger technology (DLT) refers to the protocols and supporting infrastructure that allow computers in different locations to propose and validate transactions and update records in a synchronized way across a network. The new systems of DLT are designed to function without a trusted authority. In such systems, transactions are conducted in a peer-to-peer fashion and broadcast to the entire set of participants who work to validate them in batches known as "blocks." Since the ledger of activity is organized into separate but connected blocks, this type of DLT is often referred to as "blockchain technology." *See* Morten Bech and Rodney Garratt, Central bank cryptocurrencies, BIS Quarterly Review, September 2017, at 58.

and preserving trustworthy digital records is of significant interest to those working in records and information management.[2] Because Blockchain seeks to promote the integrity of the record by having third-party validation, distributed retention, and continuous publication, the technology may be used to support accounting, auditing, reporting, medical records, and data transfer functions.

Major corporate players are making considerable investments in initiatives developing future uses for Blockchain technologies.[3] The potential of these innovations seems at once enormous and uncertain. Increasingly, legislatures have turned their attention to this area. A leader in the adoption of Blockchain technology for the management of corporate records, Delaware passed a law in August 2017 that sanctions the use of the technology for stock trading and recordkeeping by companies incorporated in the state. Delaware has been developing an automated electronic filing process to manage reporting obligations under the Uniform Commercial Code, and future applications are envisioned that allow for the management of board resolutions, voting, corporate communications, investor communications, and tracking beneficial owners.[4] Expect to see further developments in this space as Blockchain technologies and Information Governance practices continue to gain momentum and interact.

§ 29:38 Checklist for implementing an information management policy

The following is a sample checklist for those responsible for the creation and implementation of an information management policy.[1] Every company's situation is different and for this reason the list cannot be exhaustive, but it

---

[2]Victoria L. Lemieux, Trusting records: is Blockchain technology the answer?, 26:2 Records Management J. 110-139 (2016).

[3]*See* Rhys Dipshan, IBM Launches Enterprise Blockchain Accelerator Program, Legaltech News (May 24 2017), http://legaltechnews.com/printerfriendly/id=1202787253579.

[4]Ed Silverstein, Delaware Could Be Model for Other States, Even Nations, With Blockchain Program, Legaltech News (Sept. 13, 2017), http://legaltechnews.com/printerfriendly/id=1202797912416.

[Section 29:38]

[1]*See* § 29:17.

should provide a helpful summary of the major issues to be considered in developing the policy. A more detailed checklist summarizing all the topics discussed in this chapter follows at Section 29:39.

I. Understand the need for and philosophy behind an information management policy:
   a. A company must develop reasonable policies and procedures, tailored to its specific needs and circumstances, for managing its information.
   b. Companies need not and should not retain all electronic or paper information they create.
   c. Information should be maintained only as long as required by law or by business and operational considerations.
   d. An effective information management policy can result in enormous cost savings when a company becomes party to a litigation or a government investigation.
   e. An organization must establish policies and procedures that permit it to suspend routine destruction of information (both records and non-records) related to actual or reasonably anticipated litigation, government investigation, or audit.

II. Audit current practices: (§ 29:32)
   a. Engage the company's internal audit team.
   b. Involve in-house or outside counsel, or both.
   c. Involve IT personnel.
   d. Involve department representatives who work with the company's information.
   e. Evaluate the information (records and non-records) created by the company.
   f. Understand the software and hardware used by the company and their impact on information management.
   g. Evaluate the company's business and organizational structure.
   h. Review the company's current record retention schedule and information management policies, and compliance with them.
   i. Evaluate the kinds of litigation or investigations the company expects to be involved in.

III. Develop the policy:

a. Identify the records to which the policy applies.
b. Select appropriate retention periods in light of relevant considerations.
c. Include legal and regulatory requirements.
d. Address business/operational needs.
e. Identify technological implications.

IV. Implement and monitor compliance with the policy:
a. Train all personnel who work with documents under the policy.
b. Purge information according to the retention schedules.
c. Ensure migration of critical information when upgrading hardware or software.
d. Monitor compliance with the policy.
e. Implement legal holds when necessary.
f. Determine when holds will be issued.
g. Determine who has authority to issue a hold.
h. Determine who is responsible for communicating and implementing the hold.
i. Determine who is responsible for recirculating the hold or updating its recipients.
j. Define the scope of the hold.
k. Define the mechanism for implementing the hold.
l. Document the hold.
m. Remove the hold when it is no longer required.

V. Update the policy:
a. Monitor changes in applicable laws or regulations.
b. Consider how changes in corporate organization or business initiatives affect the policy.

§ 29:39 Practice checklist

The following checklist is provided to guide those responsible for the development and maintenance of the company's Information Governance strategy. Every company may define Information Governance differently and for this reason the checklist below summarizing all the topics discussed in this chapter cannot be exhaustive, but it should provide a helpful summary of the major issues to be considered in developing the strategy.

I. Introduction to Information Governance (§ 29:2)
a. Companies require an Information Governance

program which will effectively manage and control information in a legally compliant manner in order to maximize benefits and minimize risks.

b. In the development of an Information Governance program, companies should consider information ownership, management, and value.

c. Depending on a company's requirements, the scope of an Information Governance program may be narrow (records management) or broad (the governance of information.

II. Key concepts (§ 29:3)

a. Understand key Information Governance concepts.

III. Evolution of Information Governance (§ 29:4)

a. Information governance is impacted by technological developments. It has evolved from the governance of physical documents and records to electronic documents.

b. Understand the evolution from "Records Management" to "Records and Information Management" to Information Lifecycle Management.

c. Information Lifecycle Management describes policies and procedures that govern the management of data in a company from creation to destruction.

d. Companies should be aware of the nexus between Information Governance, data privacy, information security and electronic discovery.

IV. Complexities (§ 29:5)

a. Information governance is a complex, constantly evolving, and interconnected field.

b. Understand the dual nature of information.

c. Understand there are competing retention requirements and privacy obligations.

d. Distinguish between Information Governance concepts such as records management and data management.

V. Navigating the Legal and Regulatory Landscape (§ 29:6)

a. Legal research is the foundation of a legally compliant information governance program.

b. There are several legal and regulatory requirements including competing legal requirements to consider in developing an Information Governance program.

c. Companies should utilize a comprehensive legal methodology which will focus on local, regional, and global requirements.

VI. Risks of Legal Non-Compliance (§ 29:7)

a. Companies should understand that not all risks are created equal. Information security and privacy risk may outweigh other Information Governance related risks.

b. Information governance related risks discussed in this section include privacy, regulatory compliance and audits, electronic discovery, and employee training.

VII. Importance of Information Governance Strategy (§ 29:8)

a. Information governance strategy sets out the roadmap for the company to manage information assets, consists of guiding principles or rules, and defines actions and priorities.

b. Without an Information Governance strategy, a company makes tactical decisions that may not support the long-term goals of the company as they relate to the management of information.

VIII. Building the Strategy (§ 29:9)

a. The way in which a company defines Information Governance will guide the development of an Information Governance strategy.

IX. Scope of the Information Governance Program (§ 29:10)

a. It is essential for a company to properly scope and define the Information Governance program before developing the strategy.

X. Governance Model Including Executive Ownership, Leadership and Proper Delegation (§ 29:11)

a. An Information Governance model needs to be developed and deployed to lead Information Governance strategy efforts and the implementation of the strategy, and continuously improve the Information Governance program.

b. It is important to select a governance model that will fit with the company's structure.

c. The governance model should include a governing board or committee that is typically lead by some-

one with knowledge and authority to make decisions on behalf of the company on a variety of key issues.

XI. Proactive Information Management Practices (§ 29:12)

a. Companies should engage in proactive information practices such as minimizing their information footprint and focusing on security and privacy classifications.

XII. Flexibility (§ 29:13)

a. Information governance strategy promotes consistency across the company and needs to be structured in a way that allows for flexibility to comply with specific laws and regulations in each jurisdiction and different parts of the company.

XIII. Identifying Existing Information Management Challenges (§ 29:14)

a. Companies should identify existing Information Governance challenges prior to developing an Information Governance strategy. The focus should be on identifying the major issues.

b. In-house counsel can provide valuable guidance to proactively address these challenges (*e.g.*, location of workforce, cloud storage, big data, etc.).

XIV. Unearthing Issues That Need Attention When Assessing Strategic Objective (§ 29:15)

a. In the course of assessing strategic issues, company may unearth an issue that requires immediate attention due to risk or potential liability. These issues often require legal counsel involvement and attention.

XV. Incorporating Technological Solutions (§ 29:16)

a. Understand that properly managing information requires harnessing various technologies.

b. Companies need to proactively consider legal, regulatory, privacy and business requirements, not just end user functionality, before selecting the right technology for the company.

XVI. Framework for Policies and Other Directives (§ 29:17)

a. How the scope of an Information Governance program is defined will guide the policy framework by dictating the topics to be covered.

b. Understand the distinction between policy, standard, and procedure.

XVII. Communication and Training (§ 29:18)

a. Communication and training is integral to any Information Governance program.

b. Companies should employ a strategic communication and training plan to properly train employees and prioritize which employees will be trained.

XVIII. Compliance, Audit and Enforcement (§ 29:19)

a. Information governance strategy must include a compliance, audit, and enforcement plan.

XIX. Implementation Plan (§ 29:20)

a. Operationalizing the Information Governance strategy requires a methodical approach which is memorialized in a very detailed implementation plan.

b. The implementation plan should have tactical activities identified with associated timing and resource needs.

c. The senior Information Governance leadership (in which lawyers will participate) need to own the development and management of the implementation plan.

XX. Maintaining and Continuously Improving the Strategy (§ 29:21)

a. An Information Governance strategy should be developed and utilized regularly, periodically reassessed, updated as needed, and re-aligned as necessary with an organization's objectives and strategic goals.

XXI. The Governing Model (§ 29:22)

a. Information governance is a long-term strategy to govern the company's information and leverage the right people, the right resources, at the right time to execute the strategy.

b. The governing model is pivotal to the successful development and execution of the strategy.

XXII. Fostering Collaboration to Drive a Successful Information Governance Strategy (§ 29:23)

a. Every department has a shared interest in the common goal of strategically and proactively governing and managing the company's information.

b. Collaboration is the key to success of the engine driving the information governance strategy.

c. The governing model fosters collaboration in two ways:
   i. Creating entities and/or forums in which cross-functional team of associates across the company and within departments work together to understand the strategy and work together to develop the tactics to put the strategy into place.
   ii. Establishing processes connecting these entities/forums to they must work together to execute the strategy consistently.

XXIII. Identifying Key Players and Stakeholders (§ 29:24)

a. The proper management of information requires a cross-functional collaboration.
b. The success of the Information Governance program relies on identifying a cadre of associates from across the company (stakeholders and key players).

XXIV. The Governing Board/Committee Embedding Collaboration into the Strategy (§ 29:25)

a. The first key entity to create is the governing board/committee which is the strategic planning team with senior leaders across the company who are stakeholders in the governance of information.
b. The governing board/committee must embed the three cornerstones of collaboration in the strategy: transparency, accountability, and cooperation.
c. The governing board/committee in addition to developing the strategy has several other key governance responsibilities:
   i. developing the implementation plan for the Information Governance strategy;
   ii. monitoring the progress of the implementation plan;
   iii. serving as an escalation point for issues arising from implementation;
   iv. keeping the strategy current by periodically reviewing and updating it;
   v. holding the tactical teams and fellow stakeholders accountable for the continuing success of the program; and
   vi. serving as ambassadors to explain the busi-

ness and risk mitigation value of Information Governance.

XXV. The Tactical Teams that Drive Implementation of the Strategy and Ongoing Maintenance (§ 29:26)

a. The entities/forums responsible for implementing the Information Governance strategy are the tactical teams consisting of stakeholders and key players who will embed the Information Governance program into the company.

b. Tactical teams must identify, align and manage the people, processes and tools to implement the Information Governance strategy.

c. Once the strategy is implemented, the tactical teams will need to remain in place to ensure that the Information Governance program is embedded in the day to day work of the company at the department and associate level.

XXVI. The Program Office: Day-to-Day Management of the IG Program (§ 29:27)

a. The Program Office, is the team that manages the program on a daily basis and consists of Information Governance professionals with subject matter knowledge in technology, legal, compliance, information lifecycle management, and an understanding of the company's business.

XXVII. The Role of Legal Counsel in Information Governance (§ 29:28)

a. In the realm of Information Governances, legal counsel can help companies to:

1. Develop an Information Governance program that post-implementation continues to be legally compliant.
2. Develop an Information Governance program that is cost-efficient and risk-averse.
3. Develop policies and procedures to ensure that the following objectives are met.

XXVIII. The Records Retention Schedule (§ 29:29)

a. The records retention schedule is the foundation of any Information Governance program.

b. Companies should understand the philosophy, scope, planning, development and maintenance of records retention schedule.

XXIX. The Records Retention Schedule—Philosophy (§ 29:30)

a. All companies generate and use records. The retention schedule accommodates all of the company's recordkeeping requirements.

b. A records retention schedule is a policy instrument that governs the creation, retention and destruction of all the business records of a company.

XXX. The Records Retention Schedule—Scope (§ 29:31)

a. A retention schedule outlines what information must be retained for how long and when and how to dispose of it when the record is no longer required.

XXXI. The Records Retention Schedule—Planning, Development and Maintenance (§ 29:32)

a. Prior to the development of a retention schedule, a company must consider the scope of its business operations in order to determine which laws and regulations apply to the company's recordkeeping.

b. During the information gathering process on a company's records, interviews can be conducted with key stakeholders within the company or standardized questionnaires distributed to the key users of the retention schedule.

c. Companies must determine who be will be performing the legal research to ensure that the retention schedule encompasses all of the statutory requirements.

d. Companies based in the U.S. and operating globally, should reconsider using a U.S. focused records retention schedule. The U.S. schedule will not accommodate the numerous legal requirements existing in different jurisdictions in which the company operates.

e. Understand the application of legal retention requirements versus the application of limitation periods to the retention schedule.

f. Retention schedules are not static documents and must be reviewed regularly.

XXXII. Trends (§ 29:33)

a. Legal practitioners should keep focused on the horizon for technological changes and legal developments.

XXXIII. Legislating Information (§ 29:34)
- a. Legislators are regulating the various ways that information needs to be managed including retention, privacy, information security, and other aspects of information governance.

XXXIV. Cloud Storage (§ 29:35)
- a. Companies are increasingly storing their information in various cloud providers' environments because it is a cost-effective and scalable option.
- b. Legal counsel should be involved up front in vetting storage options to make sure the company's Information Governance needs are being addressed.

XXXV. Safeguarding Information with Outside Counsel (§ 29:36)
- a. Due to the copious amounts of confidential and sensitive information they hold, law firms have become prime targets of hackers.
- b. Lawyers need not only to manage what their outside law firm does with their information but also select and manage proper technology that securely augments the legal collaboration process.

XXXVI. Blockchain (§ 29:37)
- a. Blockchain seeks to promote the integrity of records by having third party validation, distributed retention, and continuous publication, the technology may be used to support accounting, auditing, reporting, medical records, and data transfer functions.
- b. Companies should be aware of blockchain related legislation.

XXXVII. Checklist for implementing a information management policy (§ 29:38)
- a. A sample checklist for those responsible for the creation and implementation of an information management policy.

